출력 일자: 2004/8/25

발송번호 : 9-5-2004-034229932
발송일자 : 2004.08.24
제출기일 : 2004.10.24

수신 : 서울특별시 강남구 역삼동 649-10 서림빌딩12층(유미특허법인)
유미특허법인 귀하

135-080

특허청
의견제출통지서

출원인 명칭 파이오니아 가부시키가이샤 (출원인코드: 519980963959)
주소 일본 도쿄도 메구로쿠 메구로 1쵸메 4반 1고

대리인 명칭 유미특허법인 외 1 명
주소 서울특별시 강남구 역삼동 649-10 서림빌딩12층(유미특허법인)

출원번호 10-2001-0022370

발명의 명칭 정보 분산 장치 및 방법, 정보 기록 매체, 및 정보 기록장치 및 방법

이 출원에 대한 심사결과 아래와 같은 거절이유가 있어 특허법 제63조의 규정에 의하여 이를 통지하오니 의견이 있거나 보정이 필요할 경우에는 상기 제출기일까지 의견서[특허법시행규칙 별지 제25호의2서식] 또는/및 보정서[특허법시행규칙 별지 제5호서식]를 제출하여 주시기 바랍니다.(상기 제출기일에 대하여 매회 1월 단위로 연장을 신청할 수 있으며, 이 신청에 대하여 별도의 기간연장 승인통지는 하지 않습니다.)

[이 유]

이 출원의 특허청구범위 제1항-제20항에 기재된 발명은 그 출원전에 이 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 아래에 지적한 것에 의하여 용이하게 발명할 수 있는 것이므로 특허법 제29조제2항의 규정에 의하여 특허를 받을 수 없습니다.

= 아 래 =

- 본원 발명은 정보 분산 장치 및 방법, 정보 기록 매체, 및 정보 기록 장치 및 방법의 기술분야에 속하는 것으로, 더욱 상세하게는, 암호화된 기록 정보를 분산하는 정보 분산 장치 및 방법, 및 분산된 기록 정보를 기록하기 위해 이용되는 정보 기록 매체, 및 정보 기록 매체에 기록 정보를 기록하기 위한 정보 기록 장치 및 방법에 관한 것이나, 이와 같은 발명은 유럽특허공보 제0802527호(1996.10.8:인용발명1)의 상세한 설명, 도면 제10도의 기재내용과; 일본특개평 제09-190667호(1997.7.22:인용발명2)의 요약, 상세한 설명(제8쪽, 제11쪽), 도면 제1도에 기재된 내용으로부터 당업자라면 용이하게 발명할 수 있는 것입니다. 즉, 본원 발명의 제1항-제20항은 인용발명1,2에 기재된 네트워크가 사용되는 타입의 광디스크 응용시스템에서의 제어실행 절차를 간편화 하며, 해적판 방지용 워치 정보를 바코드화 하여 그것을 광디스크의 특정 영역의 반사막을 제거하고 기록한 때 그 바코드형성을 용이하게 할 수 있도록 하는 광디스크의 구성수단과, 정보송신 기능을 갖는 통신매체에서 암호와 키정보를 이용하여 정보를 암호화 하여 송신하고 암호화 처리에 이용한 키 정보를 갖고 있는 정보재생장치만이 암호화 정보를 재생할 수 있도록 하는 구성수단 등으로부터 이 기술분야에서 통상의 지식을 가진 자가 기술적 구성의 곤란성 없이 용이하게 발명할 수 있습니다. 따라서 상기 발명들은 특허법 제29조 제2항에 해당됩니다.

[첨 부]
첨부 1 EP 0802527호(1997.10.22) 1부.
첨부2 일본공개특허공보 평09-190667호(1997.07.22) 1부. 끝.

출력 일자: 2004/8/25

2004.08.24

특허청 전기전자심사국

정보심사담당관실 심사관 박귀만

<<안내>>

문의사항이 있으시면 ☎ 042)481-8135 로 문의하시기 바랍니다.

특허청 직원 모두는 깨끗한 특허행정의 구현을 위하여 최선을 다하고 있습니다. 만일 업무처리과정에서 직원의 부조리행위가 있으면 신고하여 주시기 바랍니다.

▶ 홈페이지(www.kipo.go.kr)내 부조리신고센터

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-190667
(43)Date of publication of application : 22.07.1997

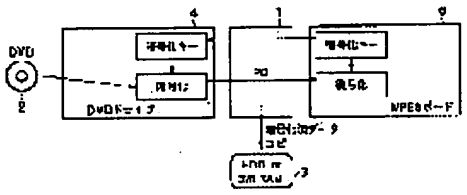
(51)Int.Cl. G11B 19/02
G06F 12/14

(21)Application number : 08-000985
(22)Date of filing : 08.01.1996

(71)Applicant : TOSHIBA CORP
(72)Inventor : NAKAMURA SEIICHI

(54) CONTROLLING METHOD AND DEVICE FOR COPYING

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system which is capable of free control of copying for every piece of information offered by recording mediums, communication mediums, etc., of a large capacity on the medium side and practical use of offered information based on reliable and legitimate copying by encoding the information transmitted from a drive to an information transmitting means by the use of key information produced by an information reproducing device(MPEG board) and by copying and reproducing the information which only an information reproducing device having the key information used in the encoding process reads through the drive.
SOLUTION: A MPEG board 6 sends the key information produced by the corresponding board to a DVD(Digital Video Disk) drive 4. The drive 4 produces encoded key information based on the above key information to encode the offered information read by the DVD 2 based on the corresponding key information and to send it to the MPEG board 6. The board 6 decodes the offered information which has been encoded by using the key information produced by the corresponding board.



LEGAL STATUS

[Date of request for examination]	25.04.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3176030
[Date of registration]	06.04.2001
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1] In the system equipped with the drive which reads the information recorded on the mass record medium, and the means recordable as an information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output A drive receives key information from an information regenerative apparatus, and carries out encryption processing of the information read from the mass record medium based on the key information concerned. For the means of signal transduction delivery and an information regenerative apparatus The duplicate control approach of the information recorded on the mass record medium characterized by carrying out decryption processing of the information which was received from the means of signal transduction, and by which encryption processing was carried out using the key information relevant to the key information published to the drive, and being able to reproduce.
[Claim 2] The drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output, In the system equipped with the means which can record the information transmitted to the means of signal transduction An information regenerative apparatus publishes key information to a drive, carry out encryption processing of the information which the drive read from the mass record medium based on the key information received from the information regenerative apparatus, and the means of signal transduction is passed. The duplicate control approach of the information recorded on the mass record medium characterized by carrying out decryption processing of the information which only the information regenerative apparatus which published key information recorded on the drive through the means of signal transduction, and being able to reproduce.
[Claim 3] In the system equipped with the drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output The key information to which a drive and an information regenerative apparatus relate mutually using random information is generated temporarily. Encipher the information which a drive outputs to the means of signal transduction using temporary key information which carried out self-generation, and the information which the information regenerative apparatus received from the means of signal transduction using temporary key information which carried out self-generation is decrypted. The duplicate control approach of the information recorded on the mass record medium characterized by having enabled playback of the information read from the drive and making improper playback of the duplicate information which once recorded the information read from the drive.
[Claim 4] In the system equipped with the drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output A drive or an information regenerative apparatus generates primary key information based on random information at least. A drive and an information regenerative apparatus carry out self-generation of the respectively temporary secondary key information based on the key information concerned. By enciphering the information which a drive outputs to the means of signal transduction using the secondary key information which carried out self-generation, and decrypting the information which the information regenerative apparatus received from the means of signal transduction using the secondary key information which carried out self-generation The duplicate control approach of the information recorded on the mass record medium characterized by having enabled playback of the information read from the drive and making playback of duplicate information improper.
[Claim 5] In the system equipped with the drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output Primary key information is generated based on the random information on a drive and an information regenerative apparatus, respectively. Deliver the key information concerned mutually and self-generation of the temporary secondary key information is carried out based on the each first key information. By enciphering the information which a drive outputs to the means of signal transduction using the secondary key information which carried out self-generation, and decrypting the information which the information regenerative apparatus received from the means of signal transduction using the secondary key information which carried out self-generation The duplicate control approach of the information recorded on the mass record medium characterized by having hidden the key information with which encryption and a decryption are presented from the means of signal transduction, and making playback of duplicate information improper.

[Claim 6] In the system equipped with the drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output Read-out of the information set from a mass record medium as the reproductive object is faced a drive. Read specific control information and the duplicate authorization level to the duplicate information which was read from the record medium concerned and was once recorded from the control information is recognized. When it is the level which duplicate authorization level permits playback of duplicate information only with a specific information regenerative apparatus, Using the key information which received the information which becomes the basis of a key from the reproduced information regenerative apparatus, and was generated based on the information concerned When it is the level which encryption processing of the information read from the mass record medium is carried out, it delivers to the means of signal transduction, and duplicate authorization level forbids playback of the duplicate information on all information regenerative apparatus, Receive information more nearly random than the reproduced information regenerative apparatus, and temporary key information is generated based on the information concerned. By the specific control information which carried out encryption processing of the information read from the mass record medium using the key information concerned, delivered to the means of signal transduction, and was recorded on the mass record medium The duplicate control approach of the information recorded on the mass record medium characterized by enabling it to control duplicate authorization of duplicate information to arbitration.
[Claim 7] The means of signal transduction is the duplicate control approach claim 1 realized by the computer apparatus or other equipments in which the informational record which or is transmitted is possible, 2, 3, 4, 5, or given in six. [information transmission]
[Claim 8] An information regenerative apparatus is the duplicate control approach claim 1 realized on the playback board which carried the MPEG decoder for MPEG1, MPEG 2, or MPEG4, 2, 3, 4, 5, or given in six.
[Claim 9] A mass record medium is the duplicate control approach claim 1 realized with the disk which carried out fixed record of the provided information including the image information compressed by MPEG1, MPEG 2, or MPEG4, 2, 3, 4, 5, or given in six.
[Claim 10] The duplicate control approach of claim 1, 2, or 3 publications with a means to match and save the key information generated with the information regenerative apparatus to duplicate information.
[Claim 11] Claim 1 which can set up key information with any value, 2, or the duplicate control approach given in three.
[Claim 12] The key information used for processing of encryption or a decryption at least is the duplicate control approach 1 by which the contents are changed, 2, 3, 4, 5, or given in six at least at reproductive initiation or every termination.
[Claim 13] An information regenerative apparatus is the duplicate control approach according to claim 1 or 2 which has the key information on the encryption associated mutually, and the key information on a decryption, and has a means to carry out encryption processing of the key information on encryption at least, and to send out to a drive.
[Claim 14] The duplicate control approach according to claim 6 that the contents of the key information used for processing of encryption or a decryption at least whenever the contents of the specific control information read from a mass record medium change are changed.
[Claim 15] Claim 1 by which encryption processing of the key information received and passed between a drive and an information regenerative apparatus is carried out on the means of signal transduction, 3, 4, 5, or the duplicate control approach given in six.
[Claim 16] The information regenerative apparatus of the mass record medium characterized by coming to prepare a means publish key information for decrypting the information received from the drive in the information regenerative apparatus equipped with the decoder which regenerates in response to the information which was recorded on the mass record medium and read with drive equipment inside, and publish to a drive the key information for enciphering the information outputted from a drive.
[Claim 17] The drive equipment of the mass record medium characterized by coming to provide a means hold in response to key information from an information regenerative apparatus in case the information recorded on the mass record medium reproduces in the drive equipment of the mass record medium which reads the information recorded on the mass record medium, and is delivered to an information regenerative apparatus, and a means encipher the information which transmits to an information regenerative apparatus based on this key information.
[Claim 18] The drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output, In the system equipped with the means which can record the information transmitted to the means of signal transduction as duplicate information The generation means of key information and a means to publish key information to a drive are formed in an information regenerative apparatus. The duplicate control unit which receives the above-mentioned key information in a drive, establishes the means which carries out encryption processing of the information read from the mass record medium based on this key information, and is characterized by the ability only of the information regenerative apparatus which published key information at the drive to reproduce duplicate information.
[Claim 19] In the system equipped with the drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output A means to generate key information is mutually established according to an individual for the information relevant to a drive and an information regenerative apparatus. A means to encipher the information outputted to a drive at the means of signal transduction using the

key information which carried out self-generation is established. The duplicate control unit of the information recorded on the mass record medium characterized by having established a means to decrypt the information received in the information regenerative apparatus from the means of signal transduction using the key information which carried out self-generation, and hiding the key information used for encryption and a decryption from the means of signal transduction.

[Claim 20] In the system equipped with the drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output A means to generate primary key information based on random information to a drive or an information regenerative apparatus at least is established. The means which carries out self-generation of the temporary secondary key information based on the above-mentioned primary key information is formed in a drive and an information regenerative apparatus. The duplicate control unit characterized by decrypting the information which enciphered the information which a drive outputs to the means of signal transduction using the secondary key information which carried out self-generation, and the information regenerative apparatus received from the means of signal transduction using the secondary key information which carried out self-generation.

[Claim 21] In the system equipped with the drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output A means to generate primary key information based on random information to each of a drive and an information regenerative apparatus, A means to generate secondary key information using the each first key information generated on the both sides is established. The duplicate control unit characterized by decrypting the information which enciphered the information which a drive outputs to the means of signal transduction using the secondary key information which carried out self-generation, and the information regenerative apparatus received from the means of signal transduction using the secondary key information which carried out self-generation.

[Claim 22] The drive which reads the information recorded on the mass record medium, and the information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output, A means to hold the key information relevant to mutual to a drive and an information regenerative apparatus in the system equipped with the means which can record the information transmitted to the means of signal transduction as duplicate information, In response to the specific control information recorded on the mass record medium, a means to judge the duplicate authorization level of the information read from a mass record medium is established. The information read to the drive from the mass record medium according to duplicate authorization level Encryption processing is carried out so that the decode processing of the duplicate information can be carried out only with an information regenerative apparatus with related key information. By or the specific control information which established the means delivered to the means of signal transduction, without carrying out encryption processing so that no information regenerative apparatus can carry out decode processing of the duplicate information, or performing encryption processing, and was recorded on the mass record medium The duplicate control unit characterized by enabling it to control duplicate authorization of duplicate information to arbitration.

[Claim 23] The duplicate control unit according to claim 22 which formed the generation means of key information, and a means to publish key information to a drive in the information regenerative apparatus, received the above-mentioned key information in the drive, established the means which carries out encryption processing of the information read from the mass record medium based on this key information, and enabled playback of duplicate information only with the specific information regenerative apparatus.

[Claim 24] A means to generate key information is mutually established according to an individual for the information relevant to a drive and an information regenerative apparatus. A means to encipher the information outputted to a drive at the means of signal transduction using the key information which carried out self-generation is established. The duplicate control unit according to claim 22 with which a means to decrypt the information received in the information regenerative apparatus from the means of signal transduction using the key information which carried out self-generation is established, and all the information regenerative apparatus could be made not to carry out decode processing of the duplicate information.

[Claim 25] The means of signal transduction is a duplicate control unit claim 18 realized by the computer apparatus or other equipments in which the informational record which or is transmitted is possible, 19, 20, 21, 22, or given in 23. [information transmission]

[Claim 26] An information regenerative apparatus is a duplicate control unit claim 18 realized on the board which carried the MPEG decoder for MPEG1, MPEG 2, or MPEG4, 19, 20, 21, 22, or given in 23.

[Claim 27] A mass record medium is a duplicate control unit claim 18 realized with the disk which carried out fixed record of the provided information including the image information compressed by MPEG1, MPEG 2, or MPEG4, 19, 20, 21, 22, 23, or given in 24.

[Claim 28] The duplicate control unit of claim 18, 22, or 23 publications with a means to match and save the key information generated with the information regenerative apparatus to duplicate information.

[Claim 29] Claim 18 which can set up key information with any value, 22, or a duplicate control unit given in 23.

[Claim 30] The key information used for processing of encryption or a decryption at least is a duplicate control unit claim 18 by which the contents are changed, 19, 20, 21, 22, 23, or given in 24 at least at reproductive initiation or every termination.

[Claim 31] An information regenerative apparatus is a duplicate control unit according to claim 18 or 22 which has

the key information on the encryption associated mutually, and the key information on a decryption, and has a means to carry out encryption processing of the key information on encryption at least, and to send out to a drive.
[Claim 32] Claim 22 by which the contents of the key information used for processing of encryption or a decryption at least whenever the contents of the specific control information read from a mass record medium change are changed, 23, or a duplicate control unit given in 24.
[Claim 33] The duplicate control unit according to claim 18, 20, 21, or 22 with which encryption processing of the key information received and passed between a drive and an information regenerative apparatus is carried out on the means of signal transduction.
[Claim 34] The information offer equipment which offers information through means of communications, and the information regenerative apparatus which receives information from information offer equipment and carries out a playback output through means of communications, In the system which comes to have the means which can record the information supplied to an information regenerative apparatus through means of communications as duplicate information An information regenerative apparatus publishes key information to information offer equipment, and encryption processing of the information transmitted to the information regenerative apparatus of an offer place based on the key information which information offer equipment received from the information regenerative apparatus is carried out. The duplicate control approach of the information offered by the communication link characterized by the ability only of the information regenerative apparatus which published key information used for encryption processing to reproduce duplicate information.
[Claim 35] The information offer equipment which offers information through means of communications, and the information regenerative apparatus which receives information from information offer equipment and carries out a playback output through means of communications, In the system equipped with the means which can record the information supplied to an information regenerative apparatus through means of communications as duplicate information The key information to which information offer equipment and an information regenerative apparatus relate mutually using random information is generated temporarily. Encipher the information which information offer equipment sends out to means of communications using temporary key information which carried out self-generation, and the information which the information regenerative apparatus received through means of communications using temporary key information which carried out self-generation is decrypted. The duplicate control approach of the information offered by the communication link characterized by having enabled informational playback received through means of communications, and making improper playback of the duplicate information which once recorded the information concerned.
[Claim 36] The information offer equipment which offers information through means of communications, and the information regenerative apparatus which receives information from information offer equipment and carries out a playback output through means of communications, In the system equipped with the means which can record the information supplied to an information regenerative apparatus through means of communications as duplicate information information offer equipment The duplicate authorization information that the authorization level of duplicate information is specified is sent out to an information regenerative apparatus. An information regenerative apparatus Recognize the authorization level of the duplicate of the information offered based on the duplicate authorization information received from information offer equipment, and when it is the authorization level which can reproduce duplicate information Deliver to an information regenerative apparatus through means of communications, without carrying out encryption processing of the information to offer, and when playback of duplicate information is possible authorization level only in a specific information regenerative apparatus Receive key information from an information regenerative apparatus, and the provided information which carried out encryption processing based on the key information concerned is delivered to an information regenerative apparatus through means of communications. When it is the authorization level which forbids playback of duplicate information The duplicate control approach of the information offered by the communication link characterized by delivering the provided information which generated temporarily the key information to which information offer equipment and an information regenerative apparatus relate mutually using random information, and carried out encryption processing based on the key information concerned to an information regenerative apparatus through means of communications.
[Claim 37] Means of communications is the duplicate control approach of the information offered by communication link claim 34 realized by the communication line connected to a computer apparatus and the equipment concerned, 35, or given in 36.
[Claim 38] The information offer equipment which offers information through means of communications, and the information regenerative apparatus which receives information from information offer equipment and carries out a playback output through means of communications, In the system equipped with the means which can record the information supplied to an information regenerative apparatus through means of communications as duplicate information A means to generate the key information on a proper at the equipment concerned is formed in an information regenerative apparatus. The duplicate control unit of the information offered by the communication link characterized by the ability only of the information regenerative apparatus which has the key information with which received key information from the information regenerative apparatus, established the encryption processing means [provided information] based on the key information concerned, and encryption processing was presented in information offer equipment to reproduce duplicate information.
[Claim 39] The information offer equipment which offers information through means of communications, and the information regenerative apparatus which receives information from information offer equipment and carries out a playback output through means of communications, In the system equipped with the means which can record the

information supplied to an information regenerative apparatus through means of communications as duplicate information A means which carries out a means to generate key information is mutually established according to an individual for the information relevant to each of information offer equipment and an information regenerative apparatus. The duplicate control unit of the information offered by the communication link which carries out encryption processing of the provided information which information offer equipment sends out to means of communications using the key information which carried out self-generation, and is characterized by decrypting the information which the information regenerative apparatus received through means of communications using the information which carried out self-generation.

[Claim 40] The information offer equipment which offers information through means of communications, and the information regenerative apparatus which receives information from information offer equipment and carries out a playback output through means of communications, A means to recognize the duplicate authorization level of the information concerned on the occasion of information offer to information offer equipment in the system equipped with the means which can record the information supplied to an information regenerative apparatus through means of communications as duplicate information, A means to deliver the information to offer to an information regenerative apparatus through means of communications, without carrying out encryption processing when duplicate authorization information is the level which permits playback of duplicate information, When duplicate authorization information is the level which only a specific information regenerative apparatus permits playback of duplicate information, Receive the key information which the reproduced information regenerative apparatus generated, and the provided information which carried out encryption processing based on the key information concerned is delivered to an information regenerative apparatus through means of communications. When duplicate authorization information is the level which does not permit playback of duplicate information The duplicate control unit of the information offered by the communication link characterized by receiving information more nearly random than the reproduced information regenerative apparatus, generating temporary key information based on the information concerned, and delivering the provided information which carried out encryption processing based on the key information concerned to an information regenerative apparatus through means of communications.

[Claim 41] Means of communications is the duplicate control unit of the information offered by communication link claim 38 realized by the computer apparatus by which the line connection was carried out to the communication line and the circuit concerned, 39, or given in 40.

[Claim 42] An information regenerative apparatus is a duplicate control unit of the information offered by the communication link according to claim 38, 39, 40, or 41 realized on the board which carried the MPEG decoder for MPEG1, MPEG 2, or MPEG4.

[Claim 43] Information offer equipment is a duplicate control unit of the information offered by communication link claim 38 which transmits provided information including the image information compressed by MPEG1, MPEG 2, or MPEG4 to an information regenerative apparatus through means of communications, 39, or given in 40.

[Claim 44] The read-out equipment which reads information from the medium which recorded provided information including image information, The computer apparatus connected to this read-out equipment, and the board which regenerates the provided information received with this computer apparatus, It is the computer system equipped with the means which can record the information passed to the computer apparatus as duplicate information. To read-out equipment A means to generate the 1st key information on arbitration with a random number, and a means to hold the 1st key information, A means to hold in response to the 2nd key information from a board, and a means to generate the 3rd key information from the 1st key information and the 2nd key information, A means to receive the 5th key information that the proper was enciphered by the board from a board, to decrypt using the 3rd key information, and to hold, A means to send out the 1st key information to a board, and the means which carries out read-out maintenance of the duplicate authorization information from a medium, The means which carries out encryption processing of the provided information read from the medium using the 3rd key information or the 5th key information according to duplicate authorization information alternatively is provided. On a board A means to generate the 2nd key information on arbitration with a random number, and a means to hold the 2nd key information, A means to send out the 2nd key information to read-out equipment, and a means to hold in response to the 1st key information from read-out equipment, A means to generate the 4th key information from the 1st key information and the 2nd key information, A means to generate the 5th of a proper, and the 6th key information on a board, and a means to encipher using the 4th key information and to send out the 5th key information to read-out equipment, A means to hold in response to duplicate authorization information from read-out equipment, and the means which carries out decryption processing of the provided information received from the computer apparatus using the 4th key information or the 6th key information according to duplicate authorization information alternatively are provided. When encryption processing is carried out using the 5th key information and decryption processing is carried out using the 6th key information, When only the board which published each key information concerned makes refreshable duplicate information on the information read from the medium, and carries out encryption processing using the 3rd key information and decryption processing is carried out using the 4th key information, The duplicate control unit characterized by enabling playback of the information read from the medium and making playback of duplicate information improper.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the duplicate control approach and duplicate control unit which are applied to information processing system with the regenerative function of the provided information which carries out the playback output of the information (provided information is called) in which compression processing was carried out by MPEG 2 etc., such as a movie and music.
[0002] This invention relates to the duplicate control approach and duplicate control unit which can control the reuse of the duplicate information at the time of recording the information recorded on mass record media, such as CD-ROM and DVD (digital video disc), as duplicate information, and reproducing by the specific control information recorded on the medium concerned.
[0003] This invention receives provided information, such as a movie and music, through means of communications, and relates to the informational duplicate control approach and informational duplicate control unit which are applied to the computer system equipped with the function which carries out the playback output of the provided information concerned and which are offered by communication link.
[0004]
[Description of the Prior Art] In the system which carries out the playback output of the information (provided information is called) in which is offered from film producing industry or music industry, for example, compression processing was carried out by MPEG 2 etc., such as a movie and music, the copy protection technique for preventing an unjust duplicate is needed.
[0005] In the system which computer-processes the high provided information of added value which was especially described above, and carries out a playback output, establishment of the reliable copy protection technique instead of the copy protection technique of extent canceled by computer processing in which an unjust duplicate can be prevented certainly is made indispensable.
[0006] This conventional seed copy protection technique recorded unjust duplicate prevention information on record media, such as CD-ROM which recorded provided information, collectively, and this unjust duplicate prevention information was read with provided information, it transmitted to the unjust duplicate arrester, and the unjust duplicate is prevented by processing duplicate prevention into provided information.
[0007] However, in such a conventional copy protection technique, the unjust duplicate of provided information on purpose will be allowed in a system configuration to which processing of duplicate prevention is not performed until the provided information currently recorded on the disk is transmitted to an unjust duplicate arrester, therefore a computer apparatus intervenes as transmission equipment between the read-out equipment of a disk, and a regenerative apparatus.
[0008] Thus, the reliable copy protection technique in which an unjust duplicate could be certainly prevented in the system by which it is placed between delivery of provided information by the computer in the former was not established, but when it was going to build the system which can incorporate and use a part of provided information for a computer alternatively especially, there was a problem of allowing an unjust duplicate for all provided information.
[0009]
[Problem(s) to be Solved by the Invention] The movie information offered by a mass record medium etc. in the former as mentioned above, In the system by which it is placed between delivery of provided information, such as music information, by the computer When it is going to build the system which the reliable copy protection technique in which an unjust duplicate can be prevented certainly is not established, but can incorporate and use a part of provided information for a computer alternatively especially, There was a problem of allowing an unjust duplicate for all provided information.
[0010] This invention was made in view of the above-mentioned actual condition, and aims at offering the reliable duplicate control approach and duplicate control unit which can prevent an unjust duplicate certainly also in the system by which it is placed between delivery of the information offered by a mass record medium etc. by the computer.
[0011] Moreover, it aims at offering the utilizable duplicate control approach and the duplicate control unit of the provided information by the reliable and always just duplicate which can control duplicate use to arbitration for every provided information by the medium side, without showing the key information use for processing of encryption and a decryption as a computer apparatus also in the system by which it is place between delivery of the

information offer by a mass record medium, communication media, etc. by the computer apparatus in this invention.
[0012]
[Means for Solving the Problem] In the system by which it is placed between delivery of the information offered by a mass record medium, communication media, etc. by the equipment which a computer etc. can duplicate process, on the equipment which a computer etc. can duplicate process, since the information read from the medium is in the condition enciphered by the specific key, this invention can control the playback propriety of duplicate information to arbitration.
[0013] Moreover, this invention is set to the system by which it is placed between delivery of the information offered by a mass record medium, communication media, etc. by the equipment which a computer etc. can duplicate process. The ** which does not show directly the key information used for processing of encryption and a decryption as the equipment which a computer etc. can duplicate process, The utilizable duplicate control approach and duplicate control unit of the provided information by playback of a reliable and always just duplicate which can control the reuse of duplicate information to arbitration for every provided information by the medium side are offered. In addition, in this invention, it has called it "playback of duplicate information" to once record the information offered by a mass record medium, communication media, etc. on storage etc., to read it, and to reproduce.
[0014] Namely, the drive which reads the information by which this invention was recorded on the mass record medium, The information regenerative apparatus which receives the information read from this drive through the means of signal transduction, and carries out a playback output, In the system equipped with the means which can record the information transmitted to the means of signal transduction as duplicate information Encryption processing is carried out using the key information which generated the information received and passed to the means of signal transduction from a drive with the information regenerative apparatus, and only an information regenerative apparatus with the key information used for encryption processing is characterized by what (that is, a time cost copy is permitted) duplicate information is [a thing] reproducible.
[0015] In the above-mentioned system a drive and an information regenerative apparatus moreover, respectively The key information mutually related based on random information is generated according to an individual. A drive By enciphering the information outputted to the means of signal transduction using the key information which carried out self-generation, and decrypting the information which the information regenerative apparatus received from the means of signal transduction using the secondary key information which carried out self-generation Without passing the key information used for cipher processing and decode processing to the means of signal transduction, playback of only an information regenerative apparatus with related key information is permitted, and it is characterized by making playback of duplicate information improper.
[0016] In the above-mentioned system, a drive and an information regenerative apparatus moreover, based on the specific control information recorded on the mass record medium When it is the level which recognizes duplicate authorization level and permits playback of duplicate information When it is the level which delivers to the means of signal transduction, without carrying out encryption processing of the information read from the drive, and permits playback of duplicate information only with a specific information regenerative apparatus After carrying out encryption processing of the information which read from the drive the information read from the drive using the key information generated with the reproduced information regenerative apparatus, When it is the level which delivers to the means of signal transduction and forbids playback of duplicate information The key information to which a drive and an information regenerative apparatus relate mutually using random information is generated temporarily. It is characterized by making improper playback of the duplicate information on all the information regenerative apparatus containing the information regenerative apparatus in which only an information regenerative apparatus with related key information carries out playback of the information read from the drive possible, and has related key information.
[0017] Moreover, the information offer equipment with which this invention offers information through means of communications and the information regenerative apparatus which receives information from information offer equipment through means of communications, and carries out a playback output, In the system equipped with the means which can record the information supplied to an information regenerative apparatus through means of communications as duplicate information Information offer equipment receives key information from an information regenerative apparatus, encryption processing of the information with which an information regenerative apparatus is provided based on the key information concerned is carried out, and it is characterized by the ability only of an information regenerative apparatus with the key information used for encryption processing to reproduce duplicate information.
[0018] In the above-mentioned system information offer equipment and an information regenerative apparatus moreover, respectively Generate the key information mutually related based on random information according to an individual, and the information with which an information regenerative apparatus is provided using the cryptographic key information in which information offer equipment carried out self-generation is enciphered. By decrypting the information which the information regenerative apparatus received from information offer equipment using the decryption key information which carried out self-generation, it is characterized by having enabled informational playback received through means of communications, and making playback of duplicate information improper.
[0019] In the above-mentioned system moreover, information offer equipment The duplicate authorization information that the authorization level of duplicate information is specified is sent out to an information regenerative apparatus. An information regenerative apparatus Recognize the authorization level of the duplicate of

the information offered based on the duplicate authorization information received from information offer equipment, and when it is the authorization level which can reproduce duplicate information Deliver to an information regenerative apparatus through means of communications, without carrying out encryption processing of the information to offer, and when playback of duplicate information is possible authorization level only in a specific information regenerative apparatus Receive key information from an information regenerative apparatus, and the provided information which carried out encryption processing based on the key information concerned is delivered to an information regenerative apparatus through means of communications. When it is the authorization level which forbids playback of duplicate information The key information to which information offer equipment and an information regenerative apparatus relate mutually using random information is generated temporarily, and it is characterized by delivering the provided information which carried out encryption processing based on the key information concerned to an information regenerative apparatus through means of communications.

[0020] Also in the system by which it is placed between delivery of the information offered by a mass record medium, communication media, etc. by having the duplicate controlling mechanism which was described above by the equipment which a computer etc. can duplicate process The system which can utilize the provided information by the reliable and always just duplicate which can control playback of duplicate information to arbitration for every provided information by the medium side can be built without showing the key information used for processing of encryption and a decryption as the equipment which a computer etc. can duplicate process.

[0021]

[Embodiment of the Invention] With reference to a drawing, the operation gestalt of this invention is explained below. Drawing 1 is the block diagram showing the fundamental system configuration in the 1st operation gestalt of this invention. Here As an object of duplicate prevention of provided information recorded on the mass storage medium (DVD2), such as a movie and music The provided information received and passed to the means of signal transduction (PC1) from a drive (DVD drive 4) by carrying out encryption processing using the key information generated within the information regenerative apparatus (MPEG board 6) The operation gestalt which only an information regenerative apparatus (MPEG board 6) with the key information which carried out encryption processing reproduces the information read by the drive (DVD drive 4), and can reproduce and to which a time cost copy is permitted is illustrated.

[0022] In drawing 1 , 1 is a computer apparatus (PC) used as a signal transduction means to deliver the provided information read by the drive to an information regenerative apparatus, it incorporates alternatively the provided information which was read by the drive here and by which duplicate authorization was carried out, memorizes it to the external storage 3, such as HDD and DVD-RAM, and enables processing of edit, proofreading, etc.

[0023] 2 is the DVD disk which recorded provided information set as the object of duplicate control, such as a movie and music. While the above-mentioned provided information carries out compression processing by MPEG 2 and is recorded on this DVD2, corresponding to this provided information, duplicate authorization information (CGMS) as shown in drawing 7 is recorded on a part of media file management information block.

[0024] 4 is drive equipment which reads the information on DVD2, and has called the DVD drive here. This DVD drive 4 receives the key information generated within the information regenerative apparatus, and has the function which carries out encryption processing of the provided information read from DVD2 using the key information concerned. The concrete example of a configuration of this function is shown in drawing 2 .

[0025] 6 is an information regenerative apparatus which receives and carries out playback output processing of the provided information read by the DVD drive 4 through a computer apparatus (PC) 1, and has called the MPEG board here. This MPEG board 6 carries an MPEG 2 decoder, decodes the provided information which was received through the computer apparatus (PC) 1 and in which compression processing was carried out by MPEG 2, and acquires a playback print-out. Furthermore, while generating key information and sending out that key information to the DVD drive 4, it has the function which carries out decryption processing of the provided information using that key information in this MPEG board 6. The concrete example of a configuration of this function is shown in drawing 2 .

[0026] In the configuration of above-mentioned drawing 1 , the MPEG board 6 holds the key information concerned as a decryption key while publishing key information generated on the board 6 concerned to the DVD drive 4.

[0027] DVD — a drive — four — the above — a key — information — using — a cryptographic key — generating — being concerned — a key — using — DVD — two — reading — having had — provided information — encryption — processing — having carried out — after — a computer apparatus — (— PC —) — one — minding — the MPEG board 6 — sending out .

[0028] The MPEG board 6 receives the provided information enciphered from the DVD drive 4 through a computer apparatus (PC) 1, and carries out decryption processing using the decryption key generated on the board concerned.

[0029] By having such a duplicate controlling mechanism, only the MPEG board 6 with the key information used for encryption processing records the information read by the DVD drive 4 as duplicate information, and can be reproduced.

[0030] That is, if the DVD drive 4 gives one kind of encryption to one kind (one [or]) of provided information, even if two or more information regenerative apparatus are connected through information-transmission equipment, the reuse of duplicate information of it will become impossible except an information regenerative apparatus with the key information with which encryption was presented.

[0031] In addition, with a concrete configuration, encryption processing is performed to the key information sent to the DVD drive 4 from the MPEG board 6. Moreover, with a concrete configuration, if exclusive control of the

duplicate by the above-mentioned operation gestalt becomes effective alternatively using the above-mentioned duplicate authorization information (CGMS) and gives an example, when b0 and b1 of CGMS are "01" in drawing 7, exclusive control of the above-mentioned duplicate will be attained.

[0032] Drawing 2 is the block diagram showing the system configuration in the 2nd operation gestalt of this invention. Here The duplicate authorization level of the copy free-lancer who enables playback of the duplicate information which once recorded the provided information read from the drive according to the duplicate authorization information (CGMS) recorded on the mass record medium to all information regenerative apparatus, The system with ****** which changes alternatively the authorization level which enables playback of the above-mentioned duplicate information only with a specific information regenerative apparatus, and the authorization level which permits playback of the above-mentioned duplicate information to no information regenerative apparatus is realized.

[0033] In drawing 2, CPU of the body of a computer with which 10 and 10A are equivalent to the computer apparatus (PC) 1 shown in drawing 1 with a body, and 10 manages system-wide control, and 10A are these system buses. Here, duplicate control processing as shown under control of CPU10 at drawing 3 thru/or drawing 6 is performed. Moreover, CPU10 incorporates alternatively the provided information which drive equipment 40 read from the information record medium 20 and by which duplicate authorization was carried out, memorizes to storage 30, and processing of edit, proofreading, etc. is enabled.

[0034] 20 is an information record medium equivalent to DVD2 shown in drawing 1, and while carrying out compression processing by MPEG 2 here and being recorded, corresponding to this provided information, duplicate authorization information (CGMS) as shown in drawing 7 is recorded on a part of media file management information block.

[0035] 30 is the storage equivalent to the external storage 3 shown in drawing 1, and preservation of duplicate information, edit, proofreading, etc. are presented with it here. 40 is drive equipment equivalent to the DVD drive 4 shown in drawing 1, and reads the information on the information record medium 20. Here, it has the code generation equipments 41 and 44, the registers 42, 43, 45, 48, and 51 in which a code key is stored, read-out equipment 46, the encryption equipments 47 and 49, and decryption equipment 50 grade, and is constituted.

[0036] Code generation equipment 41 generates a code key (1) based on the random value which used random-number-generation equipment. A register 42 holds the code key (1) which the code generator 41 generated. A register 43 holds the code key (2) received from the regenerative apparatus 60 through system bus 10A.

[0037] Code generation equipment 44 generates a code key (3) using a code key (1) and a code key (2). A register 45 holds the code key (3) which the code generator 44 generated.

[0038] Read-out equipment 46 reads the information recorded on the information record medium 20. Here, provided information, such as a movie set as the object of duplicate control and music, and each duplicate authorization information (CGMS) as shown in drawing 7 which shows the duplicate authorization level of the provided information concerned are read.

[0039] Encryption equipment 47 is sent out to a regenerative apparatus 60 through system bus 10A, without carrying out encryption processing of the provided information read from the information record medium 20 using the code key (3) stored in the register 45, or the provided information cryptographic key (5) stored in the register 51 according to duplicate authorization information (CGMS), or performing encryption processing.

[0040] A register 48 holds the duplicate authorization information (CGMS) read from the information record medium 20. Encryption equipment 49 carries out encryption processing of the duplicate authorization information (CGMS) stored in the register 48, and sends it out to a regenerative apparatus 60 through system bus 10A.

[0041] Decryption equipment 50 decrypts the provided information cryptographic key (5) of the equipment proper which was received from the regenerative apparatus 60 and by which encryption processing was carried out. A register 51 holds the cryptographic key (5) by which decryption processing was carried out with decryption equipment 50.

[0042] 60 is the regenerative apparatus of the provided information equivalent to the MPEG board 6 shown in drawing 1, it carries an MPEG decoder, decodes the provided information which was received through system bus 10A and in which compression processing was carried out by MPEG 2, and acquires a playback print-out. Here, it has the code generation equipments 61 and 64, the registers 62, 63, 65, 69, 71, and 72 in which a code key is stored, the decryption equipments 66 and 67, the MPEG 2 decoder 68, and encryption equipment 70 grade, and is constituted.

[0043] Code generation equipment 61 generates a code key (2) based on the random value which used random-number-generation equipment. A register 62 holds the code key (1) received from drive equipment 40 through system bus 10A. A register 63 holds the code key (2) generated with code generation equipment 61.

[0044] Code generation equipment 64 generates a code key (4) using a code key (1) and a code key (2). A register 65 holds the code key (4) which the code generator 64 generated.

[0045] Decryption equipment 66 decrypts the duplicate authorization information (CGMS) which was received from drive equipment 40 through system bus 10A of the body of a computer and by which encryption processing was carried out.

[0046] Decryption equipment 67 is sent out to the MPEG 2 decoder 68, without carrying out decryption processing of the provided information received from drive equipment 40 through system bus 10A of the body of a computer using the code key (4) stored in the register 65, or the provided information decryption key (6) stored in the register 72 according to the duplicate authorization information (CGMS) stored in the register 71, or performing decryption

processing.
[0047] The MPEG 2 decoder 68 carries out decoding of the provided information decrypted with decryption equipment 67, and sends out the provided information in which a playback output is possible to the display controller 80. A register 69 holds the provided information cryptographic key (5) of an equipment proper. Encryption equipment 70 carries out encryption processing of the provided information cryptographic key (5) of the equipment proper stored in the register 69, and sends it out to drive equipment 40.
[0048] A register 71 holds the duplicate authorization information (CGMS) decrypted with decryption equipment 66. A register 72 holds the provided information cryptographic key (5) of the equipment proper stored in the register 69, and the provided information decryption key (6) which makes a pair (for example, a value is common).
[0049] 80 is a display controller which carries out the display output of the provided information outputted from the MPEG 2 decoder 68 to a display 81. In addition, at least, at the time of reproductive initiation or termination, the key value of registers 45 and 65 is once cleared, and is rewritten. Moreover, the key value of registers 69 and 72 may also be the configuration rewritten at the time of initiation of not only a fixed value but playback etc.
[0050] Drawing 3 thru/or drawing 6 are flow charts which show the procedure in the 2nd operation gestalt of this invention, respectively, among these drawing 3 and drawing 4 are flow charts with which the flow chart, drawing 5 , and drawing 6 which show the setting procedure of the various key information for encryption and decryption processing show the duplicate control procedure at the time of provided information read-out, respectively, respectively.
[0051] Drawing 7 is drawing showing the information format for explaining the duplicate authorization information (CGMS) in the media file management information block recorded on the information record medium 20. Here, when b0 and b1 of CGMS are "00", playback of duplicate information is permitted to all the regenerative apparatus 60, playback of exclusive duplicate information is permitted only to the regenerative apparatus used at the time of provided information read-out when b0 and b1 were "01", and when b0 and b1 are "11", playback of duplicate information is made into disapproval to all the regenerative apparatus 60.
[0052] Here explains the actuation in the 2nd operation gestalt of this invention with reference to drawing 2 thru/or drawing 7 . First, with reference to the flow chart shown in drawing 3 and drawing 4 , setting processing of the various key information for encryption and decryption processing is explained.
[0053] In connection with the system startup according to playback directions, the code generator 41 of drive equipment 40 generates a code key (1) based on a random value (drawing 3 step 40a). The code key (1) generated from this code generator 41 is set to the register 62 of a regenerative apparatus 60 by control of CPU10 while it is held at a register 42 (drawing 3 step 10a, drawing 4 step 60a).
[0054] Moreover, the code generation equipment 61 of a regenerative apparatus 60 also generates a code key (2) based on a random value (drawing 4 step 60b). The code key (2) generated from this code generator 61 is set to the register 43 of drive equipment 40 by control of CPU10 while it is held at a register 63 (drawing 3 steps 10b and 40b).
[0055] The code generation equipment 44 of drive equipment 40 generates a code key (3) using the code key (1) stored in the register 42, and the code key (2) stored in the register 43, and sets it to a register 45 (drawing 3 step 40c).
[0056] Moreover, the code generation equipment 64 of a regenerative apparatus 60 generates a code key (4) using the code key (1) stored in the register 62, and the code key (2) stored in the register 63, and sets it to a register 65 (drawing 4 step 60c).
[0057] The read-out equipment 46 of drive equipment 40 sets duplicate authorization information (CGMS) to read-out and a register 48 from the information record medium 20 (drawing 3 step 40d). Encryption equipment 49 carries out encryption processing of the duplicate authorization information (CGMS) set to the register 48 using the code key (3) stored in the register 45 (drawing 3 step 40e.). This duplicate authorization information (CGMS) by which encryption processing was carried out is passed to the decryption equipment 66 of a regenerative apparatus 60 by control of CPU10 (drawing 3 step 10c).
[0058] Decryption equipment 66 carries out decryption processing of the duplicate authorization information (CGMS) which was received from drive equipment 40 and by which encryption processing is carried out using the code key (4) stored in the register 65, and sets it to a register 71 (drawing 4 step 60d).
[0059] The control device which is not illustrated in a regenerative apparatus 60 judges the contents of the duplicate authorization information (CGMS) stored in the register 71, and when it has recognized permitting playback of exclusive duplicate information only to the regenerative apparatus with which b0 and b1 of duplicate authorization information (CGMS) are "01", and it was used at the time of provided information read-out, it starts encryption equipment 70 (drawing 4 step 60e (Yes)).
[0060] Thereby, encryption equipment 70 carries out encryption processing of the provided information cryptographic key (5) of the equipment proper currently stored in the register 69 fixed using the code key (4) stored in the register 65 (drawing 4 step 60g).
[0061] Moreover, when b0 and b1 of duplicate authorization information (CGMS) are not "01", dummy data (null value) is generated instead of a provided information cryptographic key (5) (drawing 4 step 60f).
[0062] CPU10 transmits the dummy data replaced with the provided information cryptographic key (5) of an equipment proper or it by which encryption processing was carried out to the decryption equipment 50 in drive equipment 40 (drawing 3 step 10d).
[0063] Decryption equipment 50 decrypts the provided information cryptographic key (5) of the equipment proper

which was received from the regenerative apparatus 60 and by which encryption processing was carried out, and sets it to a register 51. By the above processing, setting processing of the various key information for encryption and decryption processing is completed.

[0064] Next, the flow chart shown in drawing 5 and drawing 6 is referred to, and the duplicate control processing at the time of provided information read-out is explained. CPU10 gives read-out directions of provided information to drive equipment 40 (drawing 5 step S1).

[0065] If read-out directions are received from CPU10, read-out equipment 46 will start the control unit which is not illustrated in drive equipment 40. Read-out equipment 46 carries out drive control of the information record medium 20, and reads provided information (MPEG 2 data) and duplicate authorization information (CGMS) from the information record medium 20 (drawing 5 step S2).

[0066] After the duplicate authorization information (CGMS) read from the information record medium 20 is stored in a register 48, it is supplied to encryption equipment 47. When encryption equipment 47 judges the contents of the duplicate authorization information (CGMS) stored in the register 48 and b0 and b1 of CGMS are "00", When encryption processing of the provided information is not carried out, but it outputs as it is (passthrough) and it is "01", Encryption processing of the provided information is carried out using the provided information cryptographic key (5) of the equipment proper stored in the register 51, and when it is "11", encryption processing of the provided information is carried out using the code key (3) stored in the register 45 (drawing 5 step S3 -S7).

[0067] The provided information (MPEG 2 data) outputted from this encryption equipment 47 is transmitted to the decryption equipment 67 in a regenerative apparatus 60 through system bus 10A (drawing 5 step S8).

[0068] If the decryption equipment 67 of a regenerative apparatus 60 receives provided information (MPEG 2 data) from the encryption equipment 47 in drive equipment 40 When the contents of the duplicate authorization information (CGMS) stored in the register 71 are judged and b0 and b1 of CGMS are "00", When decryption processing of the provided information is not carried out, but it outputs as it is (passthrough) and it is "01", Decryption processing of the provided information is carried out using the provided information cryptographic key (6) of the equipment proper stored in the register 72, and when it is "11", decryption processing of the provided information is carried out using the code key (4) stored in the register 65 (drawing 5 steps S11-S16).

[0069] After decoding of the provided information (MPEG 2 data) outputted from this decryption equipment 67 is carried out by the MPEG 2 decoder 68, it is sent to the display controller 80 and a display output is carried out to a display 81 (drawing 5 step S17).

[0070] Under the present circumstances, when b0 and b1 of duplicate authorization information (CGMS) are "00", by incorporating provided information (MPEG 2 data) to storage 30, CPU10 cannot specify a regenerative apparatus but can carry out the playback output of that duplicate information at arbitration.

[0071] moreover — a duplicate — authorization — information (CGMS) — b — zero — b — one — " — 01 — " — it is — the time — provided information (MPEG 2 data) — storage — 30 — incorporating — things — encryption — processing — offering — having had — equipment — a proper — provided information — a cryptographic key — (— five —) — a key — a pair — making — equipment — a proper — provided information — a cryptographic key — (— six —) — having — a regenerative apparatus — 60 — duplicate information — being reproducible .

[0072] In addition, even if the key value of a register 72 is rewritten by subsequent regeneration by saving duplicate information at the store 30 with the cryptographic key (6) stored in the register 72 in this case, it becomes reproducible [the duplicate information which corresponds by resetting the key information which carried out / above-mentioned / preservation to read-out and a register 72].

[0073] Moreover, since the value of a code key (4) has already changed at the time of playback although incorporated to storage 30 by making provided information (MPEG 2 data) into duplicate information when b0 and b1 of duplicate authorization information (CGMS) are "11", decryption processing cannot do the duplicate information, therefore duplicate information can be reproduced in no regenerative apparatus.

[0074] Under the present circumstances, the copy protection device which made possible precise authorization control of a more reliable arbitration amount-of-information unit is realizable by considering as the configuration which newly sets up the key value of registers 69 and 72, or the key value of registers 45 and 65 synchronizing with it whenever the contents of duplicate authorization information (CGMS) change.

[0075] Thus, it is an information offer side, it can encipher for every provided information (every title of a movie or music), and since it considered as the configuration which cannot read information easily by computer etc., it is reliable and the duplicate control of provided information with the high availability by computer processing etc. is established.

[0076] Moreover, since the information read by computer etc. can be prevented from reproducing a duplicate only with the information regenerative apparatus used at the time of read-out, it enables just use of duplicate information and can eliminate unjust use.

[0077] The system which can utilize the provided information by the reliable and always just duplicate which can control duplicate use to arbitration for every provided information by the medium side according to the operation gestalt of this invention, without showing the key information use for processing of encryption and a decryption as a computer apparatus also in the system by which it is place between delivery of the information offer by a mass record medium etc. by the computer apparatus as mention above can be build.

[0078] In addition, although mass disks which need drive equipment, such as DVD and CD-ROM, were taken for the example as an information offer medium with the above-mentioned operation gestalt, also in the system configuration to which an information offer medium exists outside through a communication line, this invention is

applicable like the above-mentioned operation gestalt. In this case, it prepares in the information offer equipment of the exterior where each component except the read-out equipment 46 in the drive equipment 40 shown in drawing 2 serves as a communication link place, and the signalling channel shown in drawing 2 with a broken line can be easily realized by transposing to a channel.

[0079] Moreover, although encryption processing was carried out, respectively and duplicate authorization information (CGMS) and the provided information cryptographic key (5) of an equipment proper are transmitted with the above-mentioned operation gestalt, it is also possible to exclude encryption processing according to the dependability which does not necessarily have to carry out encryption processing and is demanded.

[0080] Moreover, although considered as the configuration which generates primary key information based on the random information on drive equipment 40 and the news regenerative apparatus 60, respectively with the above-mentioned 2nd operation gestalt Not only in this, at least, for example either drive equipment 40 or the regenerative apparatus 60 The configuration whose drive equipment 40 and regenerative apparatus 60 generate primary key information based on random information, and carry out self-generation of the respectively temporary secondary key information based on the key information concerned in short What is necessary is just the configuration which generates temporarily the key information to which a drive and an information regenerative apparatus relate mutually using random information.

[0081] Moreover, although considered as the configuration which prepares independently the provided information cryptographic key (5) of an equipment proper, and the provided information decryption key (6) of an equipment proper, respectively, and is separately stored in registers 69 and 72 in a regenerative apparatus 60 with the above-mentioned operation gestalt What is necessary is to use key information common to the provided information cryptographic key (5) and decryption key (6) of not only this but an equipment proper, and just to be able to grasp the inputted cipher system of provided information, and the contents of the cryptographic key, in order that a regenerative apparatus 60 may, in short, carry out decryption processing of the inputted provided information.

[0082] Moreover, a duplicate is reproducible with the regenerative apparatus 60 which has the provided information cryptographic key (5) key of the equipment proper with which encryption processing was presented, and the provided information cryptographic key (6) of the equipment proper which makes a pair in the 2nd operation gestalt. Although alternatively considered as the configuration using the duplicate controlling mechanism to which only a time cost copy is permitted, and the duplicate controlling mechanism which made playback of a duplicate impossible in all regenerative apparatus For example, the configuration which chooses a copy free-lancer's duplicate authorization mode, and the duplicate authorization mode which makes playback of a duplicate impossible in all regenerative apparatus, Or the combination in duplicate authorization modes of arbitration, such as a configuration which chooses a copy free-lancer's duplicate authorization mode and the duplicate authorization mode of a time cost copy, is possible.

[0083] Moreover, although aimed at the system by which it is placed between delivery of the provided information offered by a mass record medium, communication media, etc. by the computer in the above-mentioned operation gestalt Even if it is the system configuration to which it is not directly placed between delivery of provided information by the computer irrespective of this system configuration For example, communication media with the transmitting function of the drive or provided information which reads provided information from record media, such as MD, CD-ROM, and DVD, The duplicate controlling mechanism of arbitration shown in the above-mentioned operation gestalt in the interface part between the equipment which can reproduce provided information in between the equipment which reproduces the reading data is applicable.

[0084] Moreover, although provided information in which compression processing was carried out by MPEG 2, such as a movie and music, was mentioned as the example with this operation gestalt, also in the system configuration made applicable to playback including the data in which compression processing was carried out by not only this but MPEG1 or MPEG4 etc., this invention is applicable.

[0085]

[Effect of the Invention] In the system by which it is placed between delivery of the provided information offered by a mass record medium, communication media, etc. by the equipment which a computer etc. can duplicate process according to this invention as a full account was given above The ** which does not show the key information used for processing of encryption and a decryption as the equipment which a computer etc. can duplicate process, The utilizable duplicate control approach and duplicate control unit of the provided information by the reliable and always just duplicate which can control duplicate use to arbitration for every provided information by the medium side can be offered.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The block diagram showing the fundamental system configuration in the 1st operation gestalt of this invention.
[Drawing 2] The block diagram showing the system configuration in the 2nd operation gestalt of this invention.
[Drawing 3] The flow chart which shows the procedure in the 2nd operation gestalt of this invention.
[Drawing 4] The flow chart which shows the procedure in the 2nd operation gestalt of this invention.
[Drawing 5] The flow chart which shows the procedure in the 2nd operation gestalt of this invention.
[Drawing 6] The flow chart which shows the procedure in the 2nd operation gestalt of this invention.
[Drawing 7] Drawing showing the information format for explaining the duplicate authorization information (CGMS) in the media file management information block recorded on the information record medium 20 in the operation gestalt of this invention.
[Description of Notations]
1 — Computer apparatus (PC)
2 — DVD (mass storage medium)
3 — External storage
4 — DVD drive (drive equipment)
6 — MPEG board (information regenerative apparatus)
10 — CPU
10A — System bus
20 — Information record medium
30 — Storage
40 — Drive equipment
41 44 — Code generation equipment
42, 43, 45, 48, 51 — Register
46 — Read-out equipment
47 49 — Encryption equipment
50 — Decryption equipment
60 — Regenerative apparatus
61 64 — Code generation equipment
62, 63, 65, 69, 71, 72 — Register
66 67 — Decryption equipment
68 — MPEG 2 decoder
70 — Encryption equipment.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－190667

(43)公開日　平成9年(1997)7月22日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ１１Ｂ　19/02	５０１		Ｇ１１Ｂ　19/02	５０１Ｑ	
Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｂ	

審査請求　未請求　請求項の数44　ＯＬ　（全 17 頁）

(21)出願番号　特願平8－985

(22)出願日　平成8年(1996)1月8日

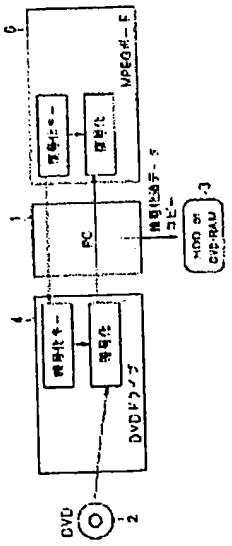
(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　中村　誠一
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　複製制御方法及び複製制御装置

(57)【要約】
【課題】本発明は、ドライブから情報伝達手段に受け渡される情報を、情報再生装置で生成したキー情報を用いて暗号化処理し、暗号化処理に用いたキー情報をもつ情報再生装置のみがドライブで読出した情報を複製し再生できるようにして、大容量記録媒体、通信媒体等の媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能なシステム が構築できることを特徴とする。
【解決手段】ＭＰＥＧボード６は当該ボードで生成したキー情報をＤＶＤドライブ４に発行する。ＤＶＤドライブ４は上記キー情報をもとにして暗号化キー情報を生成し、当該キー情報によりＤＶＤ２より読出された提供情報を暗号化処理し、ＭＰＥＧボード６に送出する。ＭＰＥＧボード６は当該ボードで生成したキー情報を用いて暗号化処理された提供情報を復号化処理する。



【特許請求の範囲】
【請求項 1】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置として記録できる手段とを備えたシステム に於いて、
ドライブは、情報再生装置よりキー情報を受け、当該キー情報をもとに大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に渡し、
情報再生装置は、情報伝達手段から受けた暗号化処理された情報をドライブに発行したキー情報に関連するキー情報により復号化処理して再生できることを特徴とした大容量記録媒体に記録された情報の複製制御方法。
【請求項 2】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を記録できる手段とを備えたシステム に於いて、
情報再生装置がドライブにキー情報を発行し、
ドライブが情報再生装置より受けたキー情報をもとに大容量記録媒体より読出した情報を暗号化処理し情報伝達手段に渡して、
ドライブにキー情報を発行した情報再生装置のみが情報伝達手段を介して記録した情報を復号化処理して再生できることを特徴とした大容量記録媒体に記録された情報の複製制御方法。
【請求項 3】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステム に於いて、
ドライブと情報再生装置がランダム な情報を用いて互いに関連するキー情報を一時的に生成し、
ドライブが、自己生成した一時的なキー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した一時的なキー情報を用いて情報伝達手段より受けた情報を復号化して、
ドライブより読出した情報の再生を可能にし、ドライブより読出した情報を一旦記録した複製情報の再生を不可にしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。
【請求項 4】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステム に於いて、
少なくともドライブ又は情報再生装置が、ランダム な情報をもとに一次キー情報を生成し、当該キー情報をもとにしてドライブ及び情報再生装置がそれぞれ一時的な二次キー情報を自己生成し、
ドライブが、自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することにより、
ドライブより読出された情報の再生を可能にし、複製情報の再生を不可にしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。
【請求項 5】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステム に於いて、
ドライブ及び情報再生装置のそれぞれが、ランダム な情報をもとに一次キー情報を生成し、当該キー情報を相互に受け渡し、その各一次キー情報をもとにして一時的な二次キー情報を自己生成し、
ドライブが、自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することにより、
暗号化及び復号化に供されるキー情報を情報伝達手段から隠して、複製情報の再生を不可にしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。
【請求項 6】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステム に於いて、
ドライブは、大容量記録媒体より、再生の対象となる情報の読出しに際して、特定の制御情報を読み、その制御情報から、当該記録媒体より読出され一旦記録された複製情報に対しての複製許可レベルを認識して、
複製許可レベルが特定の情報再生装置でのみ複製情報の再生を許可するレベルであ るとき、再生を行なう情報再生装置よりキーのもとになる情報を受け、当該情報をもとに生成したキー情報により、大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に受け渡し、
複製許可レベルが全ての情報再生装置での複製情報の再生を禁止するレベルであ るとき、再生を行なう情報再生装置よりランダム な情報を受け、当該情報をもとに一時的なキー情報を生成して、当該キー情報により大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に受け渡して、
大容量記録媒体に記録した特定の制御情報により、複製情報の複製許可を任意にコントロールできるようにしたことを特徴とする大容量記録媒体に記録された情報の複製制御方法。
【請求項 7】　情報伝達手段は、コンピュータ装置又は情報伝送装置又は伝送する情報の記録が可能な他の装置により実現される請求項 1又は2又は3又は4又は5又は6記載の複製制御方法。
【請求項 8】　情報再生装置は、ＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４を対象としたＭＰＥＧデコーダを搭載した再生ボードにより実現される請求項 1又は2又は3又は4又は5又は6記載の複製制御方法。

【請求項 9】　大容量記録媒体は、ＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４で圧縮された映像情報を含む提供情報を固定記録したディスクにより実現される請求項 １又は２又は３又は４又は５又は６記載の複製制御方法。
【請求項 10】　情報再生装置で生成したキー情報を複製情報に対応付けて保存する手段をもつ請求項 １又は２又は３記載の複製制御方法。
【請求項 11】　任意の値をもつキー情報を設定できる請求項 １又は２又は３記載の複製制御方法。
【請求項 12】　少なくとも暗号化又は復号化の処理に用いられるキー情報は、少なくとも再生の開始又は終了の都度、内容が変更される１又は２又は３又は４又は５又は６記載の複製制御方法。
【請求項 13】　情報再生装置は、互いに関連付けされた暗号化のキー情報及び復号化のキー情報をもち、少なくとも暗号化のキー情報を暗号化処理してドライブに送出する手段をもつ請求項 １又は２記載の複製制御方法。
【請求項 14】　大容量記録媒体より読出される特定の制御情報の内容が変る度に、少なくとも暗号化又は復号化の処理に用いられるキー情報の内容が変更される請求項 6記載の複製制御方法。
【請求項 15】　ドライブと情報再生装置との間で受け渡されるキー情報が情報伝達手段上に於いて暗号化処理される請求項 １又は３又は４又は５又は６記載の複製制御方法。
【請求項 16】　大容量記録媒体に記録されドライブ装置で読出された情報を受けて再生処理するデコーダを備えた情報再生装置に於いて、ドライブより受けた情報を復号化するためのキー情報を内部に発行し、ドライブより出力される情報を暗号化するためのキー情報をドライブに発行する手段を設けてなることを特徴とした大容量記録媒体の情報再生装置。
【請求項 17】　大容量記録媒体に記録された情報を読出して情報再生装置に受け渡す大容量記録媒体のドライブ装置に於いて、大容量記録媒体に記録された情報を再生する際に情報再生装置よりキー情報を受けて保持する手段と、このキー情報をもとにして情報再生装置へ転送する情報を暗号化する手段とを具備してなることを特徴とする大容量記録媒体のドライブ装置。
【請求項 18】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を複製情報として記録できる手段とを備えたシステム に於いて、
情報再生装置に、キー情報の生成手段、及びキー情報をドライブに発行する手段を設け、
ドライブに、上記キー情報を受け、このキー情報をもとに大容量記録媒体から読出した情報を暗号化処理する手段を設けて、
ドライブにキー情報を発行した情報再生装置のみが複製情報を再生できることを特徴とする複製制御装置。
【請求項 19】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステム に於いて、
ドライブ及び情報再生装置に、互いに関連する情報で個別にキー情報を生成する手段を設け、
ドライブに、自己生成したキー情報を用いて、情報伝達手段に出力する情報を暗号化する手段を設け、
情報再生装置に、自己生成したキー情報を用いて、情報伝達手段より受けた情報を復号化する手段を設けて、
暗号化及び復号化に用いるキー情報を情報伝達手段より隠したことを特徴とする大容量記録媒体に記録された情報の複製制御装置。
【請求項 20】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステム に於いて、
少なくともドライブ又は情報再生装置に、ランダム な情報をもとに一次キー情報を生成する手段を設け、
ドライブ及び情報再生装置に、上記一次キー情報をもとにして一時的な二次キー情報を自己生成する手段を設けて、
ドライブが、自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することを特徴とした複製制御装置。
【請求項 21】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステム に於いて、
ドライブ及び情報再生装置のそれぞれに、ランダム な情報をもとに一次キー情報を生成する手段と、その双方で生成された各一次キー情報を用いて二次キー情報を生成する手段とを設け、
ドライブが自己生成した二次キー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することを特徴とする複製制御装置。
【請求項 22】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を複製情報として記録できる手段とを備えたシステム に於いて、
ドライブ及び情報再生装置に、相互に関連するキー情報を保持する手段と、大容量記録媒体に記録された特定の制御情報を受けて、大容量記録媒体から読出される情報の複製許可レベルを判断する手段とを設け、
ドライブに、複製許可レベルに応じて、大容量記録媒体より読出した情報を、関連するキー情報をもつ情報再生

装置でのみ複製情報を復号処理できるように暗号化処理し、又は全ての情報再生装置が複製情報を復号処理できないように暗号化処理し、又は暗号化処理を施さずに情報伝達手段に受け渡す手段とを設けて、
大容量記録媒体に記録された特定の制御情報により、複製情報の複製許可を任意にコントロールできるようにしたことを特徴とする複製制御装置。
【請求項 23】 情報再生装置に、キー情報の生成手段、及びキー情報をドライブに発行する手段を設け、ドライブに、上記キー情報を受け、このキー情報をもとに大容量記録媒体から読出した情報を暗号化処理する手段を設けて、複製情報の再生を特定の情報再生装置でのみ可能とした請求項 22記載の複製制御装置。
【請求項 24】 ドライブ及び情報再生装置に、互いに関連する情報で個別にキー情報を生成する手段を設け、ドライブに、自己生成したキー情報を用いて、情報伝達手段に出力する情報を暗号化する手段を設け、情報再生装置に、自己生成したキー情報を用いて、情報伝達手段より受けた情報を復号化する手段を設けて、全ての情報再生装置が複製情報を復号処理できないようにした請求項 22記載の複製制御装置。
【請求項 25】 情報伝達手段は、コンピュータ装置又は情報伝送装置又は伝送する情報の記録が可能な他の装置により実現される請求項 18又は19又は20又は21又は22又は23記載の複製制御装置。
【請求項 26】 情報再生装置は、MPEG1又はMPEG2又はMPEG4を対象としたMPEGデコーダを搭載したボードにより実現される請求項 18又は19又は20又は21又は22又は23記載の複製制御装置。
【請求項 27】 大容量記録媒体はMPEG1又はMPEG2又はMPEG4で圧縮された映像情報を含む提供情報を固定記録したディスクにより実現される請求項 18又は19又は20又は21又は22又は23又は24記載の複製制御装置。
【請求項 28】 情報再生装置で生成したキー情報を複製情報に対応付けて保存する手段をもつ請求項 18又は22又は23記載の複製制御装置。
【請求項 29】 任意の値をもつキー情報を設定できる請求項 18又は22又は23記載の複製制御装置。
【請求項 30】 少なくとも暗号化又は復号化の処理に用いられるキー情報は、少なくとも再生の開始又は終了の都度、内容が変更される請求項 18又は19又は20又は21又は22又は23又は24記載の複製制御装置。
【請求項 31】 情報再生装置は、互いに関連付けされた暗号化のキー情報及び復号化のキー情報をもち、少なくとも暗号化のキー情報を暗号化処理してドライブに送出する手段をもつ請求項 18又は22記載の複製制御装置。
【請求項 32】 大容量記録媒体より読出される特定の制御情報の内容が変る度に、少なくとも暗号化又は復号化の処理に用いられるキー情報の内容が変更される請求項 22又は23又は24記載の複製制御装置。
【請求項 33】 ドライブと情報再生装置との間で受け渡されるキー情報が情報伝達手段上に於いて暗号化処理される請求項 18又は20又は21又は22記載の複製制御装置。
【請求項 34】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えてなるシステム に於いて、
情報再生装置が情報提供装置にキー情報を発行し、情報提供装置が情報再生装置より受けたキー情報をもとに提供先の情報再生装置に送信する情報を暗号化処理して、暗号化処理に用いられたキー情報を発行した情報再生装置のみが複製情報を再生できることを特徴とする通信により提供される情報の複製制御方法。
【請求項 35】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステム に於いて、
情報提供装置と情報再生装置がランダム な情報を用いて互いに関連するキー情報を一時的に生成し、情報提供装置が自己生成した一時的なキー情報を用いて通信手段に送出する情報を暗号化し、情報再生装置が自己生成した一時的なキー情報を用いて通信手段を介して受けた情報を復号化して、
通信手段を介して受けた情報の再生を可能にし、当該情報を一旦記録した複製情報の再生を不可にしたことを特徴とする通信により提供される情報の複製制御方法。
【請求項 36】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステム に於いて、
情報提供装置は、複製情報の許可レベルを指定する複製許可情報を情報再生装置に送出し、
情報再生装置は、情報提供装置より受けた複製許可情報をもとに、提供される情報の複製の許可レベルを認識して、
複製情報の再生が可能な許可レベルであ るときは、提供する情報を暗号化処理せずに通信手段を介して情報再生装置に受け渡し、
複製情報の再生が特定の情報再生装置でのみ可能な許可レベルであ るときは、情報再生装置よりキー情報を受け、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡し、
複製情報の再生を禁止する許可レベルであ るときは、情

報提供装置及び情報再生装置がランダム な情報を用いて互いに関連するキー情報を一時的に生成し、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡すことを特徴とする通信により提供される情報の複製制御方法。

【請求項 37】 通信手段は、コンピュータ装置と当該装置に接続される通信回線とにより実現される請求項 34又は35又は36記載の通信により提供される情報の複製制御方法。

【請求項 38】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステム に於いて、

情報再生装置に、当該装置に固有のキー情報を生成する手段を設け、

情報提供装置に、情報再生装置よりキー情報を受け、当該キー情報をもとに提供情報を暗号化処理する手段を設けて、

暗号化処理に供されたキー情報をもつ情報再生装置のみが複製情報を再生できることを特徴とする通信により提供される情報の複製制御装置。

【請求項 39】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステム に於いて、

情報提供装置及び情報再生装置のそれぞれに、互いに関連する情報で個別にキー情報を生成する手段する手段を設け、

情報提供装置が自己生成したキー情報を用いて通信手段に送出する提供情報を暗号化処理し、情報再生装置が自己生成した情報を用いて通信手段を介して受けた情報を復号化することを特徴とする通信により提供される情報の複製制御装置。

【請求項 40】 通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステム に於いて、

情報提供装置に、情報提供に際して当該情報の複製許可レベルを認識する手段と、複製許可情報が複製情報の再生を許可するレベルであ るとき、提供する情報を暗号化処理せずに通信手段を介して情報再生装置に受け渡す手段と、

複製許可情報が、複製情報の再生を特定の情報再生装置のみ許可するレベルであ るとき、再生を行なう情報再生装置が生成したキー情報を受け、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介して情報再生装置に受け渡し、

複製許可情報が、複製情報の再生を許可しないレベルであ るときは、再生を行なう情報再生装置よりランダム な情報を受け、当該情報をもとに一時的なキー情報を生成して、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介して情報再生装置に受け渡すことを特徴とする通信により提供される情報の複製制御装置。

【請求項 41】 通信手段は、通信回線、及び当該回線に回線接続されたコンピュータ装置により実現される請求項 38又は39又は40記載の通信により提供される情報の複製制御装置。

【請求項 42】 情報再生装置はＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４を対象としたＭＰＥＧデコータを搭載したボードにより実現される請求項 38又は39又は40又は41記載の通信により提供される情報の複製制御装置。

【請求項 43】 情報提供装置はＭＰＥＧ１又はＭＰＥＧ２又はＭＰＥＧ４で圧縮された映像情報を含む提供情報を通信手段を介し情報再生装置に送信する請求項 38又は39又は40記載の通信により提供される情報の複製制御装置。

【請求項 44】 映像情報を含む提供情報を記録した媒体から情報を読出す読出装置と、この読出装置に接続されるコンピュータ装置と、このコンピュータ装置で受取った提供情報を再生処理するボードと、コンピュータ装置に渡された情報を複製情報として記録できる手段とを備えたコンピュータシステム であ って、

読出装置には、乱数により任意の第１のキー情報を発生する手段と、第１のキー情報を保持する手段と、ボードより第２のキー情報を受けて保持する手段と、第１のキー情報と第２のキー情報から第３のキー情報を生成する手段と、ボードよりボードに固有の暗号化された第５のキー情報を受け第３のキー情報により復号化して保持する手段と、第１のキー情報をボードに送出する手段と、媒体から複製許可情報を読出し保持する手段と、複製許可情報に従い第３のキー情報又は第５のキー情報を用いて媒体から読出した提供情報を選択的に暗号化処理する手段とを具備し、

ボードには、乱数により任意の第２のキー情報を発生する手段と、第２のキー情報を保持する手段と、第２のキー情報を読出装置に送出する手段と、読出装置より第１のキー情報を受けて保持する手段と、第１のキー情報と第２のキー情報から第４のキー情報を生成する手段と、ボードに固有の第５，第６のキー情報を発生する手段と、第５のキー情報を第４のキー情報を用いて暗号化し読出装置に送出する手段と、読出装置から複製許可情報を受けて保持する手段と、複製許可情報に従い第４のキー情報又は第６のキー情報を用いてコンピュータ装置より受けた提供情報を選択的に復号化処理する手段とを具備して、

第５のキー情報を用いて暗号化処理し、第６のキー情報

を用いて復号化処理したとき、当該各キー情報を発行したボードのみが、媒体より読出した情報の複製情報を再生可能にし、
第３のキー情報を用いて暗号化処理し、第４のキー情報を用いて復号化処理したとき、媒体より読出した情報の再生を可能にし、複製情報の再生を不可にすることを特徴とした複製制御装置。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えばＭＰＥＧ２等により圧縮処理された映画、音楽等の情報（提供情報と称す）を再生出力する提供情報の再生機能をもつ情報処理システム に適用される複製制御方法及び複製制御装置に関する。
【０００２】本発明は、例えばＣＤ－ＲＯＭ、ＤＶＤ（ディジタルビデオディスク）等の大容量記録媒体に記録された情報を複製情報として記録し再生する際の複製情報の再生利用を当該媒体に記録された特定の制御情報によりコントロールできる複製制御方法及び複製制御装置に関する。
【０００３】本発明は、通信手段を介して映画、音楽等の提供情報を受信し、当該提供情報を再生出力する機能を備えたコンピュータシステム に適用される、通信により提供される情報の複製制御方法及び複製制御装置に関する。
【０００４】
【従来の技術】映画産業や音楽産業から提供される、例えばＭＰＥＧ２等により圧縮処理された、映画、音楽等の情報（提供情報と称す）を再生出力するシステム に於いては、不正な複製を防止するためのコピープロテクト技術が必要とされる。
【０００５】特に、上記したような付加価値の高い提供情報をコンピュータ処理して再生出力するシステム に於いては、コンピュータ処理で解除されてしまう程度のコピープロテクト技術ではなく、不正な複製を確実に防止することのできる信頼性の高いコピープロテクト技術の確立が必要不可欠とされる。
【０００６】従来のこの種コピープロテクト技術は、提供情報を記録したＣＤ－ＲＯＭ等の記録媒体に、不正複製防止情報を併せて記録しておき、この不正複製防止情報を提供情報とともに読出して不正複製防止装置に伝送し、提供情報に複製防止の加工を施すことにより不正複製を防止している。
【０００７】しかしながら、このような従来のコピープロテクト技術に於いては、ディスクに記録されている提供情報が不正複製防止装置に伝送されるまで複製防止の加工が施されておらず、従ってディスクの読出装置と再生装置との間に伝送装置としてコンピュータ装置が介在するようなシステム 構成に於いては提供情報の故意の不正複製を許してしまう。
【０００８】このように、従来では、提供情報の受け渡しにコンピュータが介在するシステム に於いて、不正な複製を確実に防止することのできる信頼性の高いコピープロテクト技術が確立されておらず、特に、提供情報の一部を選択的にコンピュータに取り込んで利用できるシステム を構築しようとしたとき、全ての提供情報を対象に不正な複製を許してしまうという問題があ った。
【０００９】
【発明が解決しようとする課題】上述したように、従来では、大容量記録媒体等により提供される映画情報、音楽情報等の提供情報の受け渡しにコンピュータが介在するシステム に於いて、不正な複製を確実に防止することのできる信頼性の高いコピープロテクト技術が確立されておらず、特に、提供情報の一部を選択的にコンピュータに取り込んで利用できるシステム を構築しようとしたとき、全ての提供情報を対象に不正な複製を許してしまうという問題があ った。
【００１０】本発明は上記実情に鑑みなされたもので、大容量記録媒体等により提供される情報の受け渡しにコンピュータが介在するシステム に於いても、不正な複製を確実に防止することのできる信頼性の高い複製制御方法及び複製制御装置を提供することを目的とする。
【００１１】又、本発明に於いては、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ装置が介在するシステム に於いても、コンピュータ装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能な複製制御方法及び複製制御装置を提供することを目的とする。
【００１２】
【課題を解決するための手段】本発明は、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステムに於いて、コンピュータ等の複製処理が可能な装置上では、媒体より読出された情報が特定のキーにより暗号化された状態であ るため、複製情報の再生可否を任意にコントロールできる。
【００１３】又、本発明は、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステム に於いて、コンピュータ等の複製処理が可能な装置に、暗号化及び復号化の処理に用いるキー情報を直接見せずに、媒体側で提供情報毎に複製情報の再生利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製の再生による提供情報の活用が可能な複製制御方法及び複製制御装置を提供する。尚、本発明に於いては、大容量記録媒体、通信媒体等により提供される情報を記憶装置等に一旦記録し、読出して再生することを「複製情報の再生」と称している。

【００１４】即ち、本発明は、大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置と、情報伝達手段に伝達された情報を複製情報として記録できる手段とを備えたシステム に於いて、ドライブから情報伝達手段に受け渡される情報を、情報再生装置で生成したキー情報を用いて暗号化処理し、暗号化処理に用いたキー情報をもつ情報再生装置のみが複製情報を再生できる（即ち一世代コピーを許可する）ことを特徴とする。

【００１５】又、上記システム に於いて、ドライブ及び情報再生装置のそれぞれが、ランダム な情報をもとに互いに関連するキー情報を個別に生成し、ドライブが、自己生成したキー情報を用いて情報伝達手段に出力する情報を暗号化し、情報再生装置が、自己生成した二次キー情報を用いて情報伝達手段より受けた情報を復号化することにより、暗号処理及び復号処理に用いたキー情報を情報伝達手段に漏すことなく、関連するキー情報をもつ情報再生装置のみの再生を許可し、複製情報の再生を不可にすることを特徴とする。

【００１６】又、上記システム に於いて、ドライブ及び情報再生装置が、大容量記録媒体に記録された特定の制御情報をもとに、複製許可レベルを認識し、複製情報の再生を許可するレベルであ るときは、ドライブより読出した情報を暗号化処理せずに情報伝達手段に受け渡し、複製情報の再生を特定の情報再生装置でのみ許可するレベルであ るときは、ドライブより読出した情報を、再生を行なう情報再生装置で生成したキー情報を用いてドライブより読出した情報を暗号化処理した後、情報伝達手段に受け渡し、複製情報の再生を禁止するレベルであ るときは、ドライブと情報再生装置がランダム な情報を用いて互いに関連するキー情報を一時的に生成して、関連するキー情報をもつ情報再生装置のみドライブより読出した情報の再生を可能にし、関連するキー情報をもつ情報再生装置を含む全ての情報再生装置の複製情報の再生を不可にしたことを特徴とする。

【００１７】又、本発明は、通信手段を介して情報を提供する情報提供装置と、通信手段を介して情報提供装置より情報を受け再生出力する情報再生装置と、通信手段を介して情報再生装置に供給される情報を複製情報として記録できる手段とを備えたシステム に於いて、情報提供装置が情報再生装置よりキー情報を受け、当該キー情報をもとにして情報再生装置に提供する情報を暗号化処理し、暗号化処理に用いたキー情報をもつ情報再生装置のみが複製情報を再生できることを特徴とする。

【００１８】又、上記システム に於いて、情報提供装置及び情報再生装置のそれぞれが、ランダム な情報をもとに互いに関連するキー情報を個別に生成し、情報提供装置が自己生成した暗号化キー情報を用いて情報再生装置に提供する情報を暗号化し、情報再生装置が自己生成した復号化キー情報を用いて情報提供装置より受けた情報を復号化することにより、通信手段を介して受けた情報の再生を可能にし、複製情報の再生を不可にしたことを特徴とする。

【００１９】又、上記システム に於いて、情報提供装置は、複製情報の許可レベルを指定する複製許可情報を情報再生装置に送出し、情報再生装置は、情報提供装置より受けた複製許可情報をもとに、提供される情報の複製の許可レベルを認識して、複製情報の再生が可能な許可レベルであ るときは、提供する情報を暗号化処理せずに通信手段を介して情報再生装置に受け渡し、複製情報の再生が特定の情報再生装置でのみ可能な許可レベルであるときは、情報再生装置よりキー情報を受け、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡し、複製情報の再生を禁止する許可レベルであ るときは、情報提供装置及び情報再生装置がランダム な情報を用いて互いに関連するキー情報を一時的に生成し、当該キー情報にもとづいて暗号化処理した提供情報を通信手段を介し情報再生装置に受け渡すことを特徴とする。

【００２０】上記したような複製制御機構をもつことにより、大容量記録媒体、通信媒体等により提供される情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステム に於いても、コンピュータ等の複製処理が可能な装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製情報の再生を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能なシステム が構築できる。

【００２１】

【発明の実施の形態】以下図面を参照して本発明の実施形態を説明する。図１は本発明の第１の実施形態に於ける基本的なシステム 構成を示すブロック図であ り、ここでは、大容量記憶媒体（ＤＶＤ２）に記録された、映画、音楽等の提供情報を複製防止の対象として、ドライブ（ＤＶＤドライブ４）から情報伝達手段（ＰＣ１）に受け渡される提供情報を、情報再生装置（ＭＰＥＧボード５）内で生成したキー情報を用いて暗号化処理することで、暗号化処理したキー情報をもつ情報再生装置（ＭＰＥＧボード６）のみがドライブ（ＤＶＤドライブ４）で読出した情報を複製し再生できる、一世代コピーを許可する実施形態を例示している。

【００２２】図１に於いて、１はドライブで読取った提供情報を情報再生装置に受け渡す情報伝達手段となるコンピュータ装置（ＰＣ）であ り、ここではドライブで読取った複製許可された提供情報を選択的に取り込み、ＨＤＤ、ＤＶＤ－ＲＡＭ等の外部記憶装置３に記憶して、編集、校正等の処理を可能とする。

【００２３】２は複製制御の対象となる映画、音楽等の提供情報を記録したＤＶＤディスクであ る。このＤＶＤ

2には、上記提供情報が例えばＭＰＥＧ２により圧縮処理して記録されるとともに、この提供情報に対応して、メディア・ファイル管理情報ブロックの一部に、図７に示すような複製許可情報（ＣＧＭＳ）が記録される。

【００２４】４はＤＶＤ２の情報を読取るドライブ装置であり、ここではＤＶＤドライブと称している。このＤＶＤドライブ４は、情報再生装置内で生成したキー情報を受け、当該キー情報を用いて、ＤＶＤ２より読取った提供情報を暗号化処理する機能をもつ。この機能の具体的な構成例は図２に示される。

【００２５】５はＤＶＤドライブ４で読取った提供情報をコンピュータ装置（ＰＣ）１を介して受け再生出力処理する情報再生装置であり、ここではＭＰＥＧボードと称している。このＭＰＥＧボード５は、ＭＰＥＧ２デコータを搭載し、コンピュータ装置（ＰＣ）１を介して受けた、ＭＰＥＧ２により圧縮処理された提供情報をデコードして再生出力情報を得る。更にこのＭＰＥＧボード５には、キー情報を生成し、そのキー情報をＤＶＤドライブ４に送出するとともに、そのキー情報を用いて提供情報を復号化処理する機能をもつ。この機能の具体的な構成例は図２に示される。

【００２６】上記図１の構成に於いて、ＭＰＥＧボード５は当該ボード５で生成したキー情報をＤＶＤドライブ４に発行するとともに、当該キー情報を復号化キーとして保持する。

【００２７】ＤＶＤドライブ４は上記キー情報を用いて暗号化キーを生成し、当該キーを用いて、ＤＶＤ２より読出された提供情報を暗号化処理した後、コンピュータ装置（ＰＣ）１を介しＭＰＥＧボード５に送出する。

【００２８】ＭＰＥＧボード５はＤＶＤドライブ４より暗号化された提供情報をコンピュータ装置（ＰＣ）１を介して受け、当該ボードで生成した復号化キーを用いて復号化処理する。

【００２９】このような複製制御機構を備えることにより、暗号化処理に用いたキー情報をもつＭＰＥＧボード５のみがＤＶＤドライブ４で読出した情報を複製情報として記録して再生できる。

【００３０】即ち、ＤＶＤドライブ４が、１種類（又は一つ）の提供情報に対して、１種類の暗号化を施せば、情報伝送装置を介して複数の情報再生装置が接続されていても、暗号化に供されたキー情報をもつ情報再生装置以外は複製情報の再生利用が不可能となる。

【００３１】尚、具体的な構成では、ＭＰＥＧボード５からＤＶＤドライブ４に送られるキー情報には暗号化処理が施される。又、具体的な構成では、上記実施形態による複製の排他制御が上記複製許可情報（ＣＧＭＳ）により選択的に有効となるもので、具体例を挙げると、図７に於いて、ＣＧＭＳのｂ０，ｂ１が“０１”であるとき、上記した複製の排他制御が可能となる。

【００３２】図２は本発明の第２の実施形態に於けるシステム 構成を示すブロック図であり、ここでは、大容量記録媒体に記録された複製許可情報（ＣＧＭＳ）に従い、ドライブより読出された提供情報を一旦記録した複製情報の再生をすべての情報再生装置に対して可能にするコピーフリーの複製許可レベルと、上記複製情報の再生を特定の情報再生装置でのみ可能にする許可レベルと、上記複製情報の再生をすべての情報再生装置に対して許可しない許可レベルとを選択的に切り替える機能をもつシステム を実現している。

【００３３】図２に於いて、１０及び１０Ａは図１に示すコンピュータ装置（ＰＣ）１に相当するもので、１０はシステム 全体の制御を司るコンピュータ本体のＣＰＵ、１０Ａは同システム バスである。ここではＣＰＵ１０の制御の下に、図３乃至図６に示すような複製制御処理が実行される。又、ＣＰＵ１０は、ドライブ装置４０が情報記録媒体２０より読取った複製許可された提供情報を選択的に取り込み、記憶装置３０に記憶して、編集、校正等の処理を可能とする。

【００３４】２０は図１に示すＤＶＤ２に相当する情報記録媒体であり、ここではＭＰＥＧ２により圧縮処理して記録されるとともに、この提供情報に対応して、メディア・ファイル管理情報ブロックの一部に、図７に示すような複製許可情報（ＣＧＭＳ）が記録される。

【００３５】３０は図１に示す外部記憶装置３に相当する記憶装置であり、ここでは複製情報の保存、編集、校正等に供される。４０は図１に示すＤＶＤドライブ４に相当するドライブ装置であり、情報記録媒体２０の情報を読取る。ここでは、暗号生成装置４１，４４、暗号キーを貯えるレジスタ４２，４３，４５，４８、５１、読出装置４６、暗号化装置４７，４９、復号化装置５０等を備えて構成される。

【００３６】暗号生成装置４１は、乱数発生装置を用いたランダム な値をもとに暗号キー（１）を発生する。レジスタ４２は暗号発生装置４１が発生した暗号キー（１）を保持する。レジスタ４３はシステム バス１０Ａを介して再生装置６０より受けた暗号キー（２）を保持する。

【００３７】暗号生成装置４４は暗号キー（１）と暗号キー（２）とを用いて暗号キー（３）を生成する。レジスタ４５は暗号発生装置４４が発生した暗号キー（３）を保持する。

【００３８】読出装置４６は情報記録媒体２０に記録された情報を読出す。ここでは複製制御の対象となる映画、音楽等の提供情報、及び当該提供情報の複製許可レベルを示す図７に示すような複製許可情報（ＣＧＭＳ）それぞれを読出す。

【００３９】暗号化装置４７は、情報記録媒体２０より読出した提供情報を複製許可情報（ＣＧＭＳ）に従い、レジスタ４５に貯えられた暗号キー（３）、又はレジスタ５１に貯えられた提供情報暗号化キー（５）を用いて

暗号化処理し、又は暗号化処理を施さずに、システム バス１０Ａを介して再生装置６０に送出する。

【００４０】レジスタ４８は情報記録媒体２０より読み取った複製許可情報（ＣＧＭＳ）を保持する。暗号化装置４９はレジスタ４８に貯えられた複製許可情報（ＣＧＭＳ）を暗号化処理してシステム バス１０Ａを介し再生装置６０に送出する。

【００４１】復号化装置５０は再生装置６０より受けた、暗号化処理された装置固有の提供情報暗号化キー（５）を復号化する。レジスタ５１は復号化装置５０で復号化処理された暗号化キー（５）を保持する。

【００４２】６０は図１に示すＭＰＥＧボード６に相当する提供情報の再生装置であり、ＭＰＥＧデコーダを搭載し、システム バス１０Ａを介して受けた、ＭＰＥＧ２により圧縮処理された提供情報をデコードして再生出力情報を得る。ここでは、暗号生成装置６１，６４、暗号キーを貯えるレジスタ６２，６３，６５，６９、７１，７２、復号化装置６６，６７、ＭＰＥＧ２デコーダ６８、暗号化装置７０等を備えて構成される。

【００４３】暗号生成装置６１は、乱数発生装置を用いたランダム な値をもとに暗号キー（２）を発生する。レジスタ６２はシステム バス１０Ａを介してドライブ装置４０より受けた暗号キー（１）を保持する。レジスタ６３は暗号生成装置６１で発生した暗号キー（２）を保持する。

【００４４】暗号生成装置６４は暗号キー（１）と暗号キー（２）とを用いて暗号キー（４）を生成する。レジスタ６５は暗号発生装置６４が発生した暗号キー（４）を保持する。

【００４５】復号化装置６６は、コンピュータ本体のシステム バス１０Ａを介してドライブ装置４０より受けた、暗号化処理された複製許可情報（ＣＧＭＳ）を復号化する。

【００４６】復号化装置６７はコンピュータ本体のシステム バス１０Ａを介してドライブ装置４０より受けた提供情報を、レジスタ７１に貯えられた複製許可情報（ＣＧＭＳ）に従い、レジスタ６５に貯えられた暗号キー（４）、又はレジスタ７２に貯えられた提供情報復号化キー（６）を用いて復号化処理し、又は復号化処理を施さずに、ＭＰＥＧ２デコーダ６８に送出する。

【００４７】ＭＰＥＧ２デコーダ６８は、復号化装置６７で復号化した提供情報をデコード処理して再生出力可能な提供情報を表示コントローラ８０に送出する。レジスタ６９は装置固有の提供情報暗号化キー（５）を保持する。暗号化装置７０はレジスタ６９に貯えられた装置固有の提供情報暗号化キー（５）を暗号化処理してドライブ装置４０に送出する。

【００４８】レジスタ７１は復号化装置６６で復号化された複製許可情報（ＣＧＭＳ）を保持する。レジスタ７２はレジスタ６９に貯えられた装置固有の提供情報暗号化キー（５）と対をなす（例えば値が共通する）提供情報復号化キー（６）を保持する。

【００４９】８０はＭＰＥＧ２デコーダ６８より出力された提供情報を表示装置８１に表示出力する表示コントローラである。尚、レジスタ４５，６５のキー値は、少なくとも再生の開始時又は終了時に一旦クリアされて書き替えられる。又、レジスタ６９，７２のキー値も、固定値のみでなく、例えば、再生の開始時等に書き替える構成であってもよい。

【００５０】図３乃至図６はそれぞれ本発明の第２実施形態に於ける処理手順を示すフローチャートであり、このうち、図３及び図４はそれぞれ暗号化及び復号化処理のための各種キー情報の設定処理手順を示すフローチャート、図５及び図６はそれぞれ提供情報読出し時に於ける複製制御処理手順を示すフローチャートである。

【００５１】図７は情報記録媒体２０に記録されたメディア・ファイル管理情報ブロック内の複製許可情報（ＣＧＭＳ）を説明するための情報フォーマットを示す図である。ここでは、ＣＧＭＳのｂ０，ｂ１が“００”であるとき、全ての再生装置６０に対して複製情報の再生を許可し、ｂ０，ｂ１が“０１”であるとき、提供情報読出し時に利用された再生装置のみに対して排他的な複製情報の再生を許可し、ｂ０，ｂ１が“１１”であるとき、全ての再生装置６０に対して複製情報の再生を不許可にする。

【００５２】ここで図２乃至図７を参照して本発明の第２実施形態に於ける動作を説明する。先ず、図３及び図４に示すフローチャートを参照して、暗号化及び復号化処理のための各種キー情報の設定処理を説明する。

【００５３】再生指示に従うシステム 起動に伴い、ドライブ装置４０の暗号発生装置４１はランダム な値をもとに暗号キー（１）を発生する（図３ステップ４０ａ）。この暗号発生装置４１より発生された暗号キー（１）はレジスタ４２に保持されるとともに、ＣＰＵ１０の制御で再生装置６０のレジスタ６２にセットされる（図３ステップ１０ａ、図４ステップ６０ａ）。

【００５４】又、再生装置６０の暗号生成装置６１もランダム な値をもとに暗号キー（２）を発生する（図４ステップ６０ｂ）。この暗号発生装置６１より発生された暗号キー（２）はレジスタ６３に保持されるとともに、ＣＰＵ１０の制御でドライブ装置４０のレジスタ４３にセットされる（図３ステップ１０ｂ，４０ｂ）。

【００５５】ドライブ装置４０の暗号生成装置４４はレジスタ４２に貯えられた暗号キー（１）とレジスタ４３に貯えられた暗号キー（２）とを用いて暗号キー（３）を生成しレジスタ４５にセットする（図３ステップ４０ｃ）。

【００５６】又、再生装置６０の暗号生成装置６４はレジスタ６２に貯えられた暗号キー（１）とレジスタ６３に貯えられた暗号キー（２）とを用いて暗号キー（４）

を生成し、レジスタ６５にセットする（図４ステップ６０ｃ）。

【００５７】ドライブ装置４０の読出装置４６は情報記録媒体２０より複製許可情報（ＣＧＭＳ）を読出し、レジスタ４８にセットする（図３ステップ４０ｄ）。暗号化装置４９は、レジスタ４５に貯えられた暗号キー（３）を用いて、レジスタ４８にセットされた複製許可情報（ＣＧＭＳ）を暗号化処理する（図３ステップ４０ｅ。この暗号化処理された複製許可情報（ＣＧＭＳ）はＣＰＵ１０の制御で再生装置６０の復号化装置６６に送される（図３ステップ１０ｃ）。

【００５８】復号化装置６６はレジスタ６５に貯えられた暗号キー（４）を用いて、ドライブ装置４０より受けた、暗号化処理されている複製許可情報（ＣＧＭＳ）を復号化処理し、レジスタ７１にセットする（図４ステップ６０ｄ）。

【００５９】再生装置６０内の図示しない制御装置は、レジスタ７１に貯えられた複製許可情報（ＣＧＭＳ）の内容を判断し、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“０１”で、提供情報読出し時に利用された再生装置のみに対して排他的な複製情報の再生を許可することを認識したとき、暗号化装置７０を起動する（図４ステップ６０ｅ(Yes)）。

【００６０】これにより暗号化装置７０はレジスタ６５に貯えられた暗号キー（４）を用いて、レジスタ６９に固定的に貯えられている装置固有の提供情報暗号化キー（５）を暗号化処理する（図４ステップ６０ｅ）。

【００６１】又、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“０１”でないときは、提供情報暗号化キー（５）に代わってダミーデータ（ヌル値）を生成する（図４ステップ６０ｆ）。

【００６２】ＣＰＵ１０は暗号化処理された装置固有の提供情報暗号化キー（５）又はそれに代わるダミーデータをドライブ装置４０内の復号化装置５０に転送する（図３ステップ１０ｄ）。

【００６３】復号化装置５０は再生装置６０より受けた、暗号化処理された装置固有の提供情報暗号化キー（５）を復号化してレジスタ５１にセットする。以上の処理により、暗号化及び復号化処理のための各種キー情報の設定処理が完了する。

【００６４】次に、図５及び図６に示すフローチャートを参照して、提供情報読出し時に於ける複製制御処理を説明する。ＣＰＵ１０はドライブ装置４０に対して提供情報の読出し指示を与える（図５ステップＳ１）。

【００６５】ドライブ装置４０内の図示しない制御装置は、ＣＰＵ１０より読出し指示を受けると、読出装置４６が起動する。読出装置４６は、情報記録媒体２０をドライブ制御し、情報記録媒体２０から提供情報（ＭＰＥＧ２データ）及び複製許可情報（ＣＧＭＳ）を読出す（図５ステップＳ２）。

【００６６】情報記録媒体２０から読出された複製許可情報（ＣＧＭＳ）はレジスタ４８に貯えられた後、暗号化装置４７に供給される。暗号化装置４７は、レジスタ４８に貯えられた複製許可情報（ＣＧＭＳ）の内容を判断し、ＣＧＭＳのｂ０，ｂ１が“００”であるとき、提供情報を暗号化処理せず、そのまま出力（パススルー）し、“０１”であるとき、レジスタ５１に貯えられた装置固有の提供情報暗号化キー（５）を用いて提供情報を暗号化処理し、“１１”であるとき、レジスタ４５に貯えられた暗号キー（３）を用いて提供情報を暗号化処理する（図５ステップＳ３～Ｓ７）。

【００６７】この暗号化装置４７より出力された提供情報（ＭＰＥＧ２データ）はシステム バス１０Ａを介して再生装置６０内の復号化装置６７に転送される（図５ステップＳ８）。

【００６８】再生装置６０の復号化装置６７はドライブ装置４０内の暗号化装置４７より提供情報（ＭＰＥＧ２データ）を受けると、レジスタ７１に貯えられた複製許可情報（ＣＧＭＳ）の内容を判断し、ＣＧＭＳのｂ０，ｂ１が“００”であるとき、提供情報を復号化処理せず、そのまま出力（パススルー）し、“０１”であるとき、レジスタ７２に貯えられた装置固有の提供情報暗号化キー（６）を用いて提供情報を復号化処理し、“１１”であるとき、レジスタ６５に貯えられた暗号キー（４）を用いて提供情報を復号化処理する（図５ステップＳ１１～Ｓ１６）。

【００６９】この復号化装置６７より出力された提供情報（ＭＰＥＧ２データ）はＭＰＥＧ２デコーダ６８によりデコード処理された後、表示コントローラ８０に送られて表示装置８１に表示出力される（図５ステップＳ１７）。

【００７０】この際、ＣＰＵ１０は、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“００”であるときは、提供情報（ＭＰＥＧ２データ）を記憶装置３０に取り込むことによって、その複製情報を再生装置を特定せず任意に再生出力することができる。

【００７１】又、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“０１”であるときは、提供情報（ＭＰＥＧ２データ）を記憶装置３０に取り込むことによって、暗号化処理に供された装置固有の提供情報暗号化キー（５）キーと対をなす装置固有の提供情報暗号化キー（６）をもつ再生装置６０のみが複製情報を再生できる。

【００７２】尚、この際、複製情報をレジスタ７２に貯えられた暗号化キー（６）とともに、記憶装置３０に保存しておくことにより、その後の再生処理でレジスタ７２のキー値が書き替えられても、上記保存したキー情報を読出し、レジスタ７２に再設定することで対応する複製情報の再生が可能となる。

【００７３】又、複製許可情報（ＣＧＭＳ）のｂ０，ｂ１が“１１”であるときは、提供情報（ＭＰＥＧ２デー

タ）を複製情報として記憶装置３０に取り込んでも、再生時に暗号キー（４）の値が既に変化していることから、その複製情報を復号化処理ができず、従って全ての再生装置に於いて複製情報を再生できない。

【００７４】この際、複製許可情報（ＣＧＭＳ）の内容が切り替わる度に、それに同期してレジスタ６９，７２のキー値、又はレジスタ４５，６５のキー値を新たに設定する構成とすることにより、より信頼性の高い、任意情報量単位の緻密な許可制御を可能としたコピープロテクト機構が実現できる。

【００７５】このように、情報提供側で、提供情報毎に（映画や音楽のタイトル毎に）暗号化を施すことができ、コンピュータなどで容易に情報を読み出せない構成としたことから、信頼性の高い、かつコンピュータ処理等による利用度の高い、提供情報の複製制御が確立される。

【００７６】又、コンピュータなどで読み出された情報は、読み出し時に利用された情報再生装置のみでしか複製の再生できないようにすることができることから、複製情報の正当な利用を可能にし、不当な利用を排除できる。

【００７７】上述したように本発明の実施形態によれば、大容量記録媒体等により提供される情報の受け渡しにコンピュータ装置が介在するシステム に於いても、コンピュータ装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能なシステム が構築できる。

【００７８】尚、上記した実施形態では、情報提供媒体として、ドライブ装置を必要とするＤＶＤ、ＣＤ－ＲＯＭ等の大容量ディスクを例に採ったが、情報提供媒体が例えば通信回線を介して外部に存在するシステム 構成に於いても本発明を上記実施形態と同様に適用できる。この際は、図２に示すドライブ装置４０内の読出装置４６を除く各構成要素が通信先となる外部の情報提供装置に設けて、図２に破線で示す信号路を通信路に置き換えることで容易に実現できる。

【００７９】又、上記した実施形態では、複製許可情報（ＣＧＭＳ）、及び装置固有の提供情報暗号化キー（５）をそれぞれ暗号化処理して転送しているが、必ずしも暗号化処理する必要はなく、要求される信頼性に応じて暗号化処理を省くことも可能である。

【００８０】又、上記した第２実施形態では、ドライブ装置４０及び再生装置６０のそれぞれが、ランダム な情報をもとに一次キー情報を生成する構成としているが、これに限らず、例えば少なくともドライブ装置４０又は再生装置６０のいずれか一方が、ランダム な情報をもとに一次キー情報を生成し、当該キー情報をもとにしてドライブ装置４０及び再生装置６０がそれぞれ一時的な二次キー情報を自己生成する構成等、要は、ドライブと情報再生装置がランダム な情報を用いて互いに関連するキー情報を一時的に生成する構成であればよい。

【００８１】又、上記した実施形態では、再生装置６０に於いて、装置固有の提供情報暗号化キー（５）と、装置固有の提供情報復号化キー（６）とをそれぞれ独立して設け、別個にレジスタ６９，７２に貯える構成としたが、これに限らず装置固有の提供情報暗号化キー（５）と復号化キー（６）とに共通のキー情報を用いてもよく、要は再生装置６０が、入力された提供情報を復号化処理するために、入力された提供情報の暗号化方式と暗号化キーの内容を把握できればよい。

【００８２】又、第２実施形態に於いては、暗号化処理に供された装置固有の提供情報暗号化キー（５）キーと対をなす装置固有の提供情報暗号化キー（６）をもつ再生装置６０のみにより複製を再生できる、一世代コピーのみを許可する複製制御機構と、全ての再生装置に於いて複製の再生を不能にした複製制御機構とを選択的に用いる構成としているが、例えばコピーフリーの複製許可モードと、全ての再生装置に於いて複製の再生を不能にする複製許可モードとを選択する構成、又は、コピーフリーの複製許可モードと、一世代コピーの複製許可モードとを選択する構成等、任意の複製許可モードの組み合わせが可能である。

【００８３】又、上記実施形態に於いては、大容量記録媒体、通信媒体等により提供される提供情報の受け渡しにコンピュータが介在するシステム を対象としているが、このシステム 構成に拘らず、提供情報の受け渡しにコンピュータが直接介在しないシステム 構成であっても、例えばＭＤ、ＣＤ－ＲＯＭ、ＤＶＤ等の記録媒体より提供情報を読み取るドライブ又は提供情報の送信機能をもつ通信媒体と、その読み取りデータを再生する装置との間に於いて提供情報の複製が可能な装置間のインタフェース部分に於いて、上記実施形態に示す任意の複製制御機構を適用することができる。

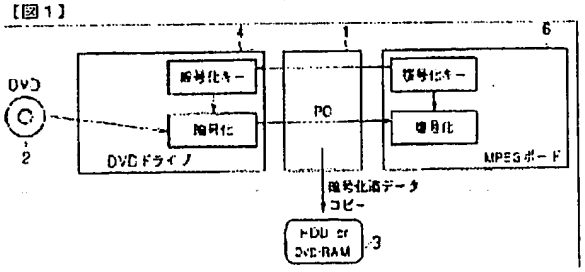
【００８４】又、この実施形態では、ＭＰＥＧ２により圧縮処理された映画、音楽等の提供情報を例に挙げたが、これに限らず、ＭＰＥＧ１又はＭＰＥＧ４等により圧縮処理されたデータを含め再生対象とするシステム 構成に於いても本発明を適用できる。

【００８５】

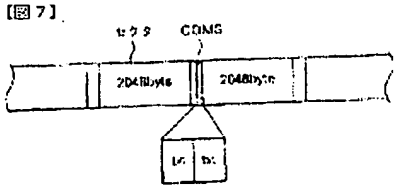
【発明の効果】以上詳記したように本発明によれば、大容量記録媒体、通信媒体等により提供される提供情報の受け渡しにコンピュータ等の複製処理が可能な装置が介在するシステム に於いて、コンピュータ等の複製処理が可能な装置に暗号化及び復号化の処理に用いるキー情報を見せずに、媒体側で提供情報毎に複製利用を任意にコントロールできる、信頼性の高い、かつ常に正当な複製による提供情報の活用が可能な複製制御方法及び複製制御装置が提供できる。

【図面の簡単な説明】
【図１】本発明の第１の実施形態に於ける基本的なシステム 構成を示すブロック図。
【図２】本発明の第２の実施形態に於けるシステム 構成を示すブロック図。
【図３】本発明の第２実施形態に於ける処理手順を示すフローチャート。
【図４】本発明の第２実施形態に於ける処理手順を示すフローチャート。
【図５】本発明の第２実施形態に於ける処理手順を示すフローチャート。
【図６】本発明の第２実施形態に於ける処理手順を示すフローチャート。
【図７】本発明の実施形態に於ける情報記録媒体２０に記録されたメディア・ファイル管理情報ブロック内の複製許可情報（ＣＧＭＳ）を説明するための情報フォーマットを示す図。
【符号の説明】
１…コンピュータ装置（ＰＣ）
２…ＤＶＤ（大容量記憶媒体）
３…外部記憶装置
４…ＤＶＤドライブ（ドライブ装置）
６…ＭＰＥＧボード（情報再生装置）
１０…ＣＰＵ
１０Ａ…システム バス
２０…情報記録媒体
３０…記憶装置
４０…ドライブ装置
４１，４４…暗号生成装置
４２，４３，４５，４８，５１…レジスタ
４６…読出装置
４７，４９…暗号化装置
５０…復号化装置
６０…再生装置
６１，６４…暗号生成装置
６２，６３，６５，６９、７１，７２…レジスタ
６６，６７…復号化装置
６８…ＭＰＥＧ２デコーダ
７０…暗号化装置。

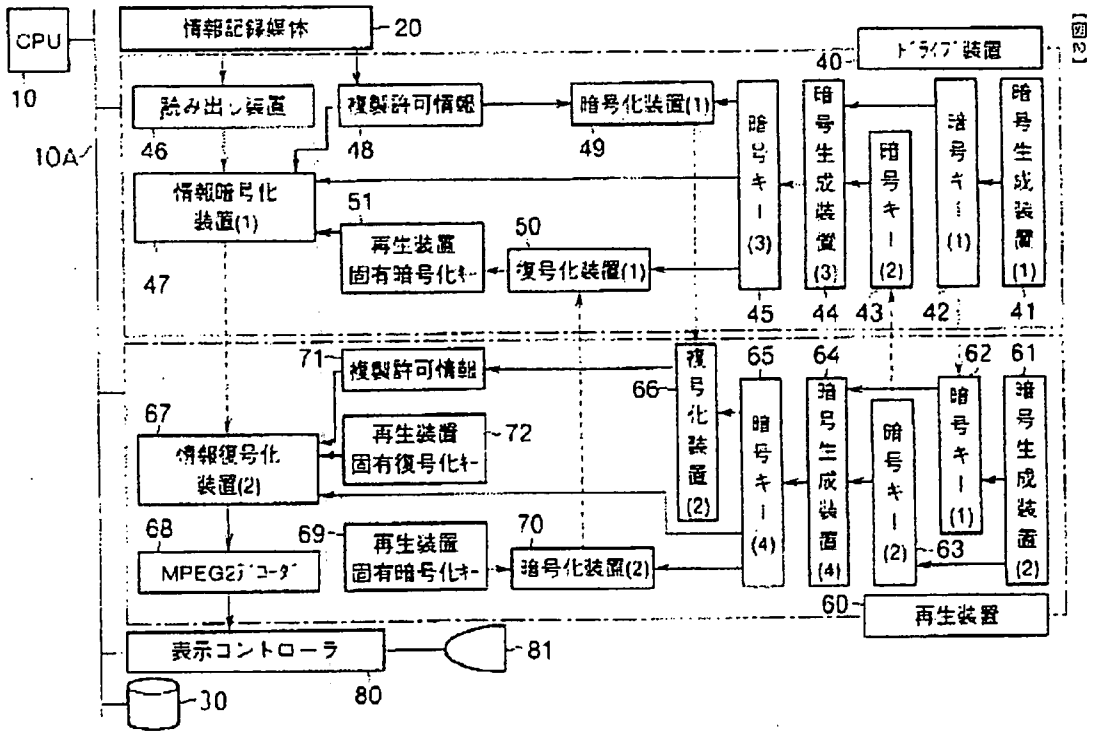
【図１】



【図７】

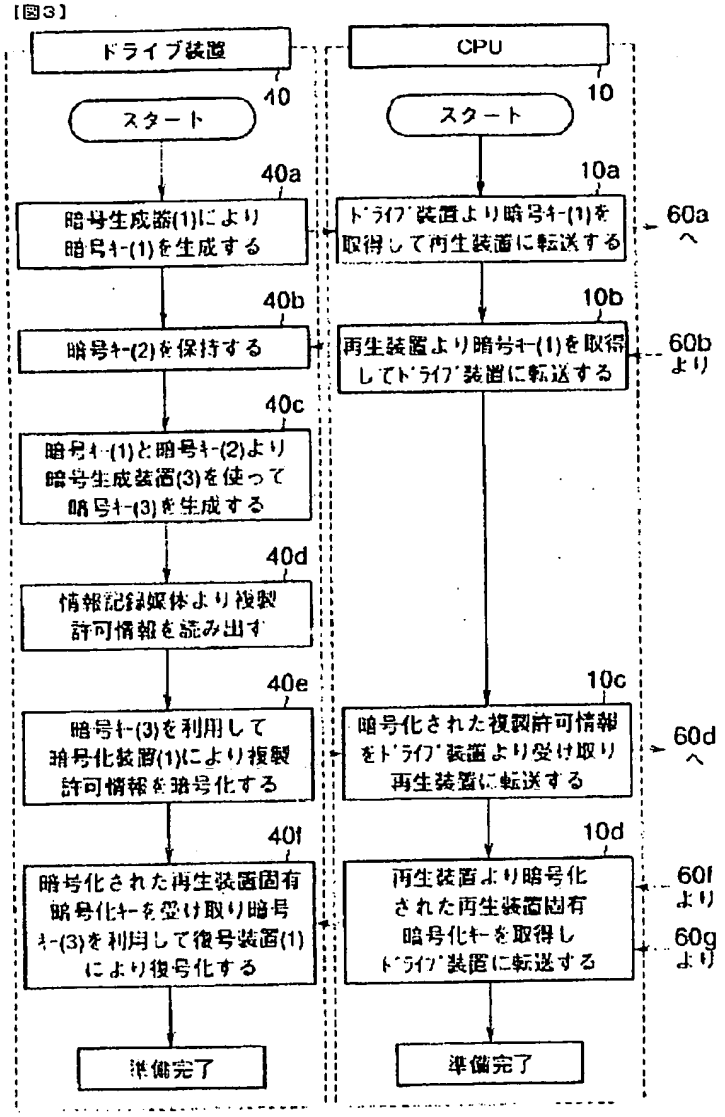


(CGMS)
(b0,b1= "00" (複製の再生可)
"01" (複製を作成したときに使用した装置でのみ複製の再生可)
"11" (複製の再生不可)

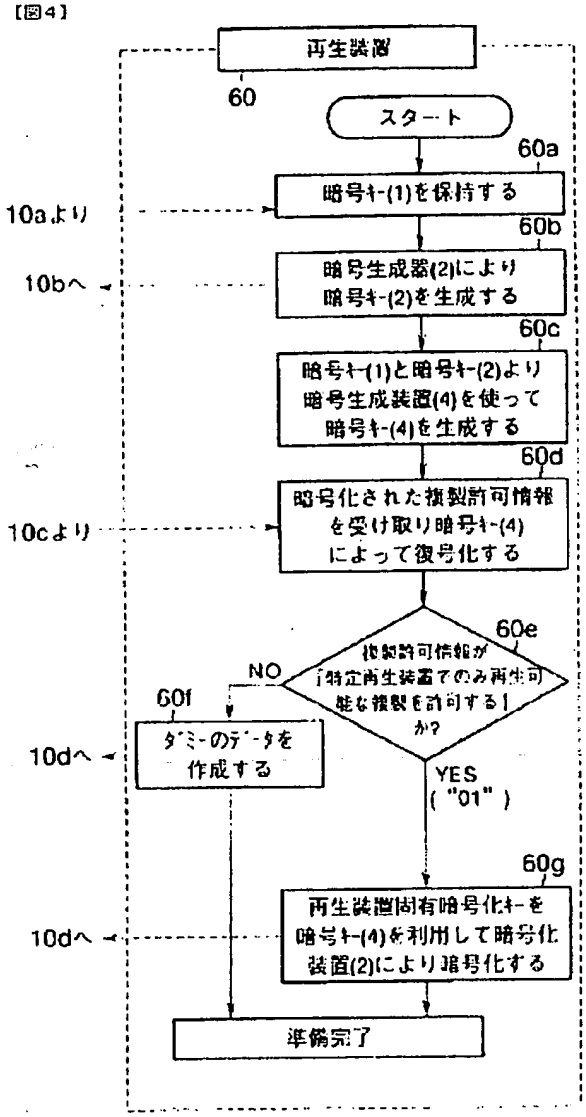

CPU
10
10A
情報記録媒体
20
読み出し装置
46
複製許可情報
48
暗号化装置(1)
49
情報暗号化装置(1)
47
51
再生装置固有暗号化キー
50
復号化装置(1)
ドライブ装置
40
暗号キー(3)
45
暗号生成装置(3)
44
暗号キー(2)
43
暗号キー(1)
42
暗号生成装置(1)
41
複製許可情報
71
67
情報復号化装置(2)
再生装置固有復号化キー
72
68
MPEG2デコーダ
69
再生装置固有暗号化キー
70
暗号化装置(2)
復号化装置(2)
66
65
暗号キー(4)
64
暗号生成装置(4)
62
暗号キー(2)
63
61
暗号生成装置(2)
暗号キー(1)
再生装置
60
表示コントローラ
80
81
30

【図2】

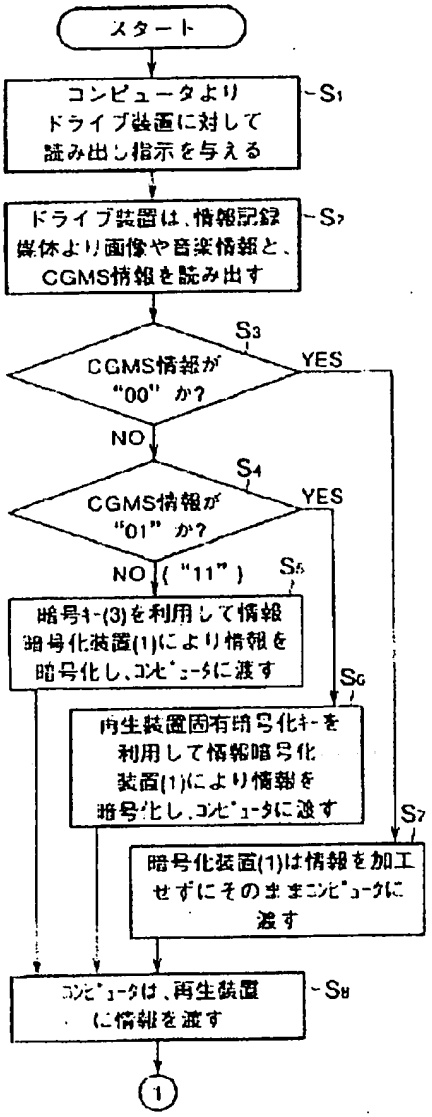
【図3】


ドライブ装置
CPU
40
10
スタート
スタート
40a
10a
暗号生成器(1)により暗号ｷｰ(1)を生成する
ﾄﾞﾗｲﾌﾞ装置より暗号ｷｰ(1)を取得して再生装置に転送する
60a へ
40b
10b
暗号ｷｰ(2)を保持する
再生装置より暗号ｷｰ(1)を取得してﾄﾞﾗｲﾌﾞ装置に転送する
60b より
40c
暗号ｷｰ(1)と暗号ｷｰ(2)より暗号生成装置(3)を使って暗号ｷｰ(3)を生成する
40d
情報記録媒体より複製許可情報を読み出す
40e
10c
暗号ｷｰ(3)を利用して暗号化装置(1)により複製許可情報を暗号化する
暗号化された複製許可情報をﾄﾞﾗｲﾌﾞ装置より受け取り再生装置に転送する
60d へ
40f
10d
暗号化された再生装置固有暗号化ｷｰを受け取り暗号ｷｰ(3)を利用して復号装置(1)により復号化する
再生装置より暗号化された再生装置固有暗号化ｷｰを取得しﾄﾞﾗｲﾌﾞ装置に転送する
60f より
60g より
準備完了
準備完了

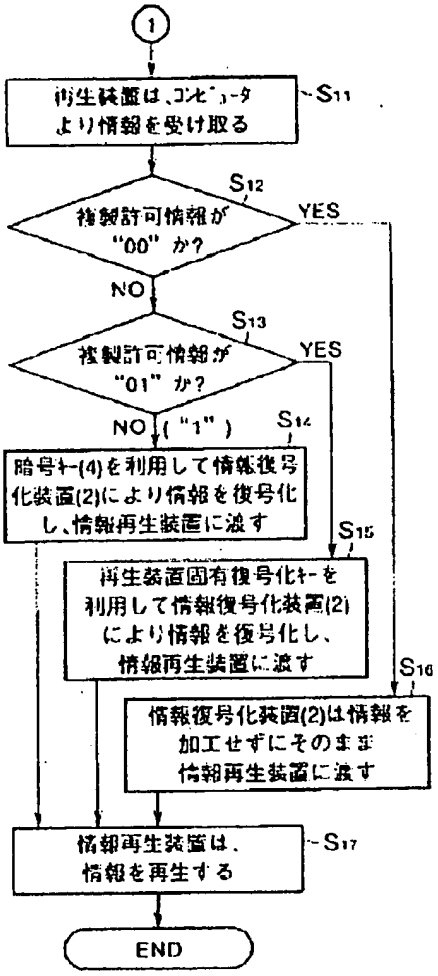
【図4】


再生装置
60
スタート
60a
暗号ｷｰ(1)を保持する
10aより
60b
暗号生成器(2)により
暗号ｷｰ(2)を生成する
10bへ
60c
暗号ｷｰ(1)と暗号ｷｰ(2)より
暗号生成装置(4)を使って
暗号ｷｰ(4)を生成する
60d
暗号化された複製許可情報
を受け取り暗号ｷｰ(4)
によって復号化する
10cより
60e
複製許可情報が
「特定再生装置でのみ再生可
能な複製を許可する」
か?
NO
60f
ﾀﾞﾐｰのﾃﾞｰﾀを
作成する
10dへ
YES
("01")
60g
再生装置固有暗号化ｷｰを
暗号ｷｰ(4)を利用して暗号化
装置(2)により暗号化する
10dへ
準備完了

【図5】


スタート
コンピュータより
ドライブ装置に対して
読み出し指示を与える
S1
ドライブ装置は、情報記録
媒体より画像や音楽情報と、
CGMS情報を読み出す
S2
CGMS情報が
"00" か?
S3
YES
NO
CGMS情報が
"01" か?
S4
YES
NO ("11")
S5
暗号ｷｰ(3)を利用して情報
暗号化装置(1)により情報を
暗号化し、ｺﾝﾋﾟｭｰﾀに渡す
S6
再生装置固有暗号化ｷｰを
利用して情報暗号化
装置(1)により情報を
暗号化し、ｺﾝﾋﾟｭｰﾀに渡す
S7
暗号化装置(1)は情報を加工
せずにそのままｺﾝﾋﾟｭｰﾀに
渡す
ｺﾝﾋﾟｭｰﾀは、再生装置
に情報を渡す
S8
1

【図6】


1
再生装置は、ｺﾝﾋﾟｭｰﾀ
より情報を受け取る
S11
複製許可情報が
"00" か?
S12
YES
NO
複製許可情報が
"01" か?
S13
YES
NO ("1")
S14
暗号ｷｰ(4)を利用して情報復号
化装置(2)により情報を復号化
し、情報再生装置に渡す
S15
再生装置固有復号化ｷｰを
利用して情報復号化装置(2)
により情報を復号化し、
情報再生装置に渡す
S16
情報復号化装置(2)は情報を
加工せずにそのまま
情報再生装置に渡す
情報再生装置は、
情報を再生する
S17
END

【手続補正書】
【提出日】平成８年１月１０日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項１
【補正方法】変更
【補正内容】
【請求項１】　大容量記録媒体に記録された情報を読出すドライブと、このドライブより読出された情報を情報伝達手段を介して受け再生出力する情報再生装置とを備えたシステムに於いて、
ドライブは、情報再生装置よりキー情報を受け、当該キー情報をもとに大容量記録媒体より読出した情報を暗号化処理して情報伝達手段に渡し、
情報再生装置は、情報伝達手段から受けた暗号化処理された情報をドライブに発行したキー情報に関連するキー情報により復号化処理して再生できることを特徴とした大容量記録媒体に記録された情報の複製制御方法。